UNIVERSIDADE ESTADUAL PAULISTA JÚLIO DE MESQUITA FILHO
CÂMPUS DE SÃO JOÃO DA BOA VISTA
PROGRAMA DE PÓS-GRADUAÇÃO EM ENGENHARIA ELÉTRICA

THIAGO DE ANDRADE BRAGAGNOLLE

Rede de Feistel e modo de operação CTR adaptados à criptografia de sinais em banda base

São João da Boa Vista
2020

THIAGO DE ANDRADE BRAGAGNOLLE

Rede de Feistel e modo de operação CTR adaptados à criptografia de sinais em banda base

Versão original

Dissertação apresentada à Universidade Estadual Paulista Júlio de Mesquita Filho – Câmpus de São João da Boa Vista para obtenção do título de Mestre em Engenharia Elétrica pelo programa de Pós-graduação em Engenharia Elétrica

Área de concentração: Automação e Sistemas Eletrônicos

Orientador: Prof. Dr. Marcelo Luís Francisco Abbade

São João da Boa Vista

2020

B813r

Bragagnolle, Thiago de Andrade
Rede de Feistel e modo de operação CTR adaptados à criptografia de sinais em banda base / Thiago de Andrade Bragagnolle. -- São João da Boa Vista, 2020
52 p.

Dissertação (mestrado) - Universidade Estadual Paulista (Unesp), Câmpus Experimental de São João da Boa Vista, São João da Boa Vista
Orientador: Marcelo Luís Francisco Abbade

1. Comunicações ópticas. 2. Segurança de sistemas. 3. Criptografia. I. Título.

Sistema de geração automática de fichas catalográficas da Unesp. Biblioteca do Câmpus Experimental de São João da Boa Vista. Dados fornecidos pelo autor(a).

Essa ficha não pode ser modificada.

Agradecimentos

Em primeiro lugar, agradeço a Deus por estar sempre cuidando de mim, por ter me proporcionado esta oportunidade de aprendizado e por me guiar nos melhores caminhos.

À toda a minha família, por me incentivar nos momentos difíceis, quando por muitas vezes não pude estar presente para poder me dedicar aos estudos. Agradeço especialmente a minha futura esposa Maria Beatriz Lourenço Bertholucci, pelo apoio e compreensão incondicional que sempre me deu.

Ao professor Doutor Marcelo Luís Francisco Abbade, por me orientar e incentivar a deixar meu trabalho o melhor possível.

Resumo

BRAGAGNOLLE, Thiago de Andrade. **Rede de Feistel e modo de operação CTR adaptados à criptografia de sinais em banda base**. 2020. 52 f. Dissertação (Mestrado em Engenharia Elétrica) – Câmpus Experimental de São João da Boa Vista, Universidade Estadual Paulista Júlio de Mesquita Filho, São João da Boa Vista, 2020.

Um dos conceitos relativos à segurança da informação é a confidencialidade. Este conceito diz sobre o quanto uma informação é restrita e somente está disponível a usuários autorizados. Algoritmos de encriptação promovem características de confidencialidade ao sistema de comunicação. Dentre diversos algoritmos disponíveis, um deles é a rede de Feistel. Neste algoritmo, uma mesma função é aplicada repetidas vezes, normalmente estruturada em número de rodadas ou ciclos. Entretanto, as redes de Feistel são um método determinístico, sendo conveniente que estas mensagens passem por algum processo adicional, que promova certa aleatoriedade ao sistema. Isso é feito por meio de modos de operação. Algoritmos de encriptação e modos de operação podem ser aplicados em diferentes camadas do modelo de referência (O*pen Systems for Interconnection*, OSI), sendo, nas camadas de dados, amplamente utilizados em padrões comerciais e, na camada física, um assunto que ainda está sendo pesquisado. O objetivo deste trabalho é apresentar uma nova proposta de criptografia de sinais em banda base para sistemas de comunicação. Esta técnica consiste em: (i) submeter o espectro de um sinal a um algoritmo de rede de Feistel adaptada a sinais, (ii) aplicar as funções próprias, que envolvem adição de fases aleatórias, que são as chaves criptográficas, e deslocamentos de posições das amostras do espectro, (iii) disponibilizar no final da rede de Feistel um sinal de saída encriptado, (iv) adicionar às fases do sinal original, preservando suas amplitudes, as fases do sinal encriptado disponibilizado pela rede de Feistel, sendo este um dos processos que caracteriza o modo de operação. Com isso, transfere-se a encriptação promovida pela rede de Feistel à mensagem desejada. Os resultados obtidos demonstram que com a utilização de 11 rodadas na rede de Feistel, proporcionou-se à mensagem encriptada as características de difusão, confusão e segurança semântica, além de não penalizar de forma significativa a recuperação da mensagem em ambientes com ruído aditivo branco e gaussiano (AWGN). Também foi observado que esta técnica permite o reuso de chaves criptográficas entre blocos. No melhor de nosso conhecimento, esta proposta de criptografia de sinais nunca havia sido antes publicada na literatura.

Palavras-chave: Criptografia de sinais. Segurança da informação. Redes de Feistel. Modos de operação. Processamento digital de sinais

Abstract

BRAGAGNOLLE, Thiago de Andrade. **Feistel cipher and CTR mode of operation adapt to signal base band cryptography**. 2020 52 f. Dissertation (Master of Electrical Engineering) – Campus São João da Boa Vista, São Paulo State University, São João da Boa Vista, 2020.

One of the concepts related to information security is confidentiality. This principle states about how restrict is an information and it is only available for authorized users. Encryption algorithms promote confidentiality features to communication systems. Among several available algorithms, one of them is the Feistel cipher. On this algorithm, a specific function is applied repeatedly, usually quantified in rounds or cycles. Due to the fact that the Feistel cipher is a deterministic methodology, it is convenient that these messages undergo an additional process in order to promote certain randomness to the system. This is made by means of modes of operation. Encryption algorithms and modes of operation can be applied in different layers of the Open Systems for Interconnection (OSI) reference model. In data layers, these algorithms are widely used in commercial standards. In physical layers, they are still under investigation. The aim of this study is to present a new signal base band cryptography proposal. This technique consists in (i) submit one spectrum signal to a Feistel cipher algorithm which is adapted to signals, (ii) apply the specific functions, involving random phase addition, that are the cryptographic keys, and spectrum samples position shifts, (iii) provide, in the end of the Feistel cipher, an output encrypted signal, (iv) add to the phases of the original signal, preserving their amplitudes, the phases of the encrypted signal provided by the Feistel cipher, the latter being one of the process that characterizes the mode of operation. The encryption process provided by the Feistel cipher is, thus transferred to the original message. The results illustrate that by using 11 rounds in the Feistel cipher, the encrypted message displayed characteristics of diffusion, confusion and semantic security, besides that, it did not significantly penalize the message recovery when in additive white gaussian noise channels. It was also observed that this technique allows the cryptography keys reuse among blocks. In the best of our knowledge, this proposal of cryptography signals has never been published before.

Key-words: Cryptography signal. Information security. Feistel cipher. Modes of operation. Digital signal process.

Lista de figuras

Figura 1 – Modelo de referência para interconexão de sistemas abertos (Open Systems for Interconnection, OSI) 13
Figura 2 - (a) Processo de encriptação de um bloco. (b) Processo de desencriptação de um bloco 22
Figura 3 - Tiny Encryption Algorithm (TEA) 24
Figura 4 - Modo de Operação CTR. (a) Processo de encriptação. (b) Processo de desencriptação. 26
Figura 5 - Proposta de processo de encriptação. (a) Diagrama geral. (b) Detalhe do Bloco de encriptação. (c) Detalhe função F_1 com as chaves K_0 e K_1. (d) Detalhe função F_1 com as chaves K_2 e K_3 28
Figura 6 - Proposta de processo de desencriptação. 30
Figura 7 - Diagrama de blocos do código 32
Figura 8 - Rede de Feistel com diferentes quantidades de rodadas 35
Figura 9 - Análise da BER da mensagem encriptada em função do número de rodadas da rede de Feistel 36
Figura 10 - Difusão provida pela rede de Feistel em função do número de rodadas 36
Figura 11 - Confusão provida pela rede de Feistel em função do número de rodadas 37
Figura 12 - Situação B2B, constelação e histogramas dos dados dos eixos real e imaginário (a) Sinal original (b) Sinal encriptado (c) Sinal desencriptado 39
Figura 13 – Resultados em um canal AWGN com SNR de 13 dB, constelação e histogramas dos dados dos eixos real e imaginário (a) Sinal original (b) Sinal encriptado (c) Sinal desencriptado. 39
Figura 14 - BER da mensagem desencriptada em função da SNR sem o modo de operação CTR 40
Figura 15 - Situação B2B, constelação e histogramas dos dados dos eixos real e imaginário (a) Sinal original (b) Sinal encriptado (c) Sinal desencriptado. 42

Figura 16 - Resultados em um canal AWGN com SNR de 13 dB, constelação e histogramas dos dados dos eixos real e imaginário (a) Sinal original (b) Sinal encriptado (c) Sinal desencriptado. 42
Figura 17 - Constelação do sinal desencriptado para diferentes valores de SNR 43
Figura 18 - BER em função da SNR com e sem criptografia 43
Figura 19 - Análise da difusão do algoritmo. 44
Figura 20 - Análise da confusão do algoritmo. 45
Figura 21 - Análise da segurança semântica do algoritmo. 46

Lista de abreviaturas e siglas

AWGN	Ruído aditivo gaussiano e branco
BER	Taxa de erro de bit
BPSK	Modulação por deslocamento de fase binária
B2B	Back-to-back
CTR	Counter
DES	Data encryption standard
DSP	Processamento digital de sinais
FEC	Correção de erros a frente
FFT	Transformada rápida de *Fourier*
FPGA	Field Programmable Gate Array
OFDM	Orthogonal frequency division multiplexing
OSI	Interconexão de Sistemas Abertos
PON	Redes ópticas passivas
QAM	Modulação por amplitude em quadratura
QPSK	Chaveamento por deslocamento de fase em quadratura
QKD	Distribuição de chave quântica
RCF	Filtro cosseno-levantado
RC5	Rivest Cipher 5
RSA	River-Shamir-Adleman
SNR	Relação sinal-ruído
TEA	Tiny Encryption Algorithm
XOR	Ou-exclusivo

Lista de símbolos

R_x	Taxa de símbolo
r	*Roll-off*
x	Número inteiro
F	Função de Feistel
F_1	Função de Feistel baseada no TEA
K_i	I-ésima chave criptográfica 0
θ	Fase
L_i	Bits da metade esquerda da informação de entrada da i-ésima rodada.
R_i	Bits da metade direita da informação de entrada da i-ésima rodada.

Sumário

1. Introdução 12

1.1 Criptografia de dados 13

1.2 Mecanismos de segurança na camada física 15

1.2.1 Esteganografia de sinais 15

1.2.2 Troca de chaves por meio da camada física 16

1.2.3 Criptografia de sinais 17

1.3 Contribuições 20

1.4 Organização da dissertação 21

2. Algoritmos de encriptação e Modo de operação CTR 22

2.1 Rede de Feistel 22

2.2 Tiny Encryption Algorithm (TEA) 23

2.3 Modo de Operação *Counter* (CTR) 25

3. Proposta de algoritmo de encriptação 28

3.1 Descrição da técnica 28

3.2 Descrição das simulações 31

4. Resultados 34

4.1 Análise para a definição da quantidade de rodadas na rede de Feistel 34

4.2 Desempenho sem o modo de operação CT 38

4.3 Desempenho da técnica 41

4.3.1 Análise para situação B2B e canal AWGN 41

4.3.2 Confidencialidade: Difusão, confusão e segurança semântica 44

5. Conclusão 47

Lista de publicações 48

Referências 49

1. Introdução

A segurança em sistemas de comunicação pode ser avaliada a partir de alguns conceitos, como: confidencialidade, integridade e disponibilidade. A confidencialidade de um sistema diz sobre o quanto a informação é restrita e está disponível apenas para receptores autorizados [1]. Se receptores não autorizados interceptarem a comunicação e não serem capazes de interpretar a mensagem, significa que o sistema de comunicação proporciona confidencialidade. A integridade está relacionada ao quanto a mensagem original é preservada após os processos de transmissão e recepção [1]. Se a mensagem se mantem sem alterações, o sistema utilizado proporciona integridade. A disponibilidade está relacionada com o quanto o sistema e seus recursos se mantem disponíveis para os usuários autorizados quando necessário. Um sistema robusto e preparado contra eventuais fatores que ameacem sua continuidade, possui características de disponibilidade.

Algoritmos de encriptação fornecem características de confidencialidade a sistemas de comunicação. Seu princípio de funcionamento estabelece que a informação original seja modificada, de forma que, a princípio, não seja possível sua recuperação não intencional ou de pessoas não autorizadas. A modificação da mensagem original é realizada com a aplicação de uma série de funções e de chaves criptográficas, que geram a informação criptografada. O receptor autorizado da informação, tendo posse da chave criptográfica, aplica as funções necessárias para recuperação da informação original.

A confidencialidade do algoritmo de encriptação pode ser avaliada por meio de conceitos como difusão, confusão e segurança semântica. O conceito de difusão está relacionado com o quanto uma informação unitária da mensagem original gera impacto sobre toda a mensagem criptografada [1]. Um bom algoritmo de encriptação deve ter sensibilidade suficiente para que pequenas mudanças na informação original gerem impacto significativo na informação criptografada. Para o atendimento do conceito de confusão, deve existir uma relação não direta e complexa entre a mensagem criptografada e a chave [1]. A segurança semântica estabelece que a mensagem criptografada não deve

revelar nada sobre a mensagem original. Mesmo que a mensagem original seja sempre a mesma, as mensagens criptografadas deverão ser sempre diferentes para que o algoritmo seja semanticamente seguro.

O processo de criptografia pode ser aplicado sobre dados ou sobre sinais. Na Subseção 1.1 será abordado o tema criptografia de dados. Na Seção 1.2 serão apresentados os mecanismos de segurança aplicados na camada física, deste as diferentes formas de prover sua confidencialidade, até métodos promissores de criptografia de sinais.

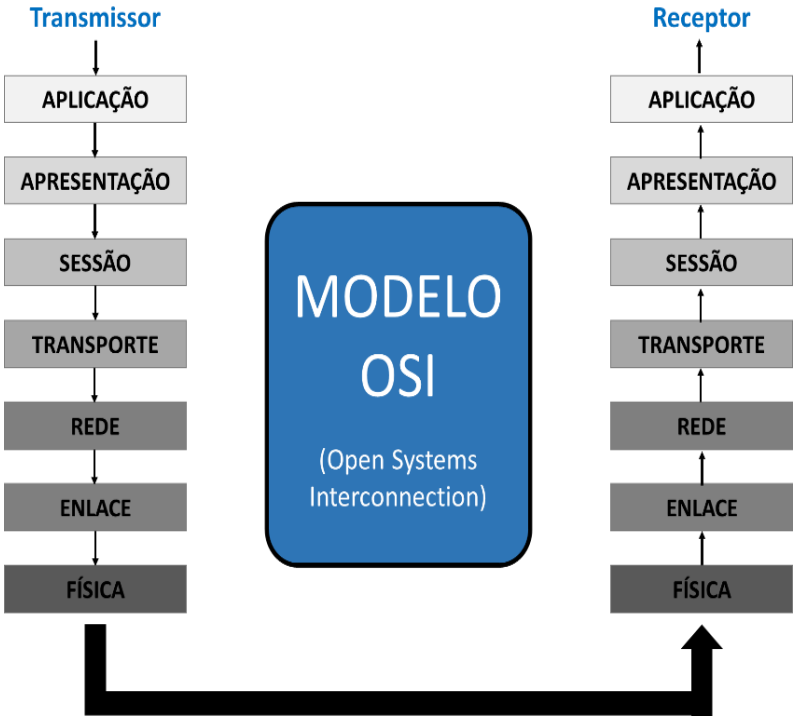

Figura 1 – Modelo de referência para interconexão de sistemas abertos (Open Systems for Interconnection, OSI)

1.1 Criptografia de dados

De acordo com o modelo de referência para interconexão de sistemas abertos (*Open Systems for Interconnection*, OSI), que é apresentado na Figura 1, existem sete camadas para padronização de redes de comunicação, sendo elas: aplicação¸ apresentação, sessão, transporte, rede, enlace e física. A

criptografia de dados é aplicada nas seis camadas superiores. Operações são aplicadas sobre os bits que constituem a mensagem. Em um exemplo que o conteúdo da mensagem é uma sequência de bits, estes seriam submetidos as operações envolvendo a chave criptográfica, de forma a modificar a sequência de bits da mensagem original, criando uma mensagem encriptada. É comum a utilização de operações lógicas como parte do processo de encriptação. O receptor, tendo a mensagem encriptada e a chave, realiza as operações necessárias para recuperar a mensagem original. A chave utilizada na recuperação da mensagem é uma informação confidencial, sendo necessário utilizar um método adequado para sua transmissão segura ao receptor. Duas estratégias amplamente utilizadas para troca de chaves são Diffie-Hellman e River-Shamir-Adleman (RSA) [2].

Outro aspecto a ser considerado na criptografia de dados é que sua aplicação pode ser realizada sobre bits individuais ou sobre um conjunto de bits. Estes métodos são chamados de criptografia de fluxo e criptografia de blocos, respectivamente. Na criptografia de fluxo, cada bit, símbolo ou byte da mensagem original é encriptado individualmente, não dependendo do restante da mensagem [3]. Na criptografia de blocos, os bits da mensagem original são divididos em conjuntos de uma determinada quantidade de bits. Desta forma, os blocos de bits são submetidos ao algoritmo de encriptação. Um aspecto positivo muito importante da criptografia de blocos é que existem diferentes formas de organizar as interações entre os blocos, as chaves e eventuais informações adicionais. Estas diferentes formas de interação são chamadas de modos de operação. A utilização de modos de operação pode permitir que, uma única chave seja utilizada para encriptar vários blocos. A vantagem deste aspecto é que o envio da chave pode acontecer a uma taxa de transmissão mais baixa comparada à taxa utilizada na transmissão do sinal.

Uma das formas de criptografia de dados existentes é baseada na solução de sistemas caóticos de acordo com a proposta de Matthews [4], que vem sendo amplamente investigado desde sua publicação. Neste método, uma chave é trocada inicialmente entre o transmissor e o receptor. Esta chave corresponde as condições iniciais que são utilizadas para a solução de um determinado sistema caótico localizado no transmissor e no receptor. A solução destas

equações gera a chave que é usada para encriptar o primeiro bloco. A seguir, a partir da chave calculada para encriptar o primeiro bloco, as equações do sistema caótico são resolvidas novamente, sendo obtida uma nova chave para encriptar o segundo bloco. Este procedimento se repete até quando for conveniente. Existem certas críticas sobre a aplicação prática desta técnica como, por exemplo, a dificuldade de análise do sistema, sua ineficiência e problemas de reprodutibilidade. Estas críticas foram publicadas em [5] e foram reforçadas em [6]. Embora exista uma diferença de 14 anos entre as referências [5] e [6], os autores da referência [6] alegam que as críticas continuam válidas. Atualmente, a criptografia de dados baseada em sistemas caóticos não é utilizada em padrões comerciais.

Diferente da criptografia de dados, a criptografia de sinais é aplicada sobre a camada física do modelo de referência OSI. Devido a sua aplicação ser sobre o sinal, a segurança é promovida para todas as demais camadas do modelo de referência OSI. Na Subseção 1.2, serão apresentadas algumas das maneiras possíveis de se utilizar a criptografia de sinais. Porém antes, será apresentado uma alternativa à criptografia que também promove confidencialidade à comunicação e métodos utilizados para a troca de chaves por meio da camada física.

1.2 Mecanismos de segurança na camada física

1.2.1 Esteganografia de sinais

A esteganografia é um método de promover a confidencialidade por meio da ocultação da informação. Propostas que utilizam este método foram apresentadas em [7] e [8]. A esteganografia não é classificada como uma forma de criptografia, uma vez que o sinal original não é modificado. Seu método consiste na transmissão de sinais com uma potência inferior ao nível de ruído, tornando-os ocultos. Porém, uma desvantagem observada nesta técnica é a vulnerabilidade do sinal sobre degradações devido à baixa potência utilizada na transmissão. Por exemplo, um sinal trafegando pelo canal na mesma frequência do sinal esteganografado, prejudicaria a recuperação da mensagem.

1.2.2 Troca de chaves por meio da camada física

Existem várias abordagens para a troca de chaves entre o transmissor e o receptor utilizando-se de propriedades da camada física. Dentre estas possibilidades, destaca-se a criptografia quântica devido ao seu alto nível de segurança. As bases desta estratégia foram propostas por Bennet [9] e por Ekert [10]. Em ambas propostas, fundamentos da mecânica quântica são usados em protocolos de distribuição de chaves. O conjunto desses fundamentos e protocolos garantem que a simples ação de espionagem de intrusos seja detectada pelo transmissor e pelo receptor.

Estas tecnologias estão sendo intensivamente pesquisadas desde que foram propostas. Na referência [11] é demonstrado como a distribuição de chaves quânticas (*quantum key distribution*, QKD) pode ser integrado a canais clássicos de comunicação óptica. Na referência [12] é apresentado um equipamento comercial que faz QKD por um enlace de até 75 km de fibra óptica. Os autores da referência [13] propõem a utilização de uma rede global de satélites para fazer QKD.

A criptografia quântica não tem seu uso limitado apenas para a troca de chaves, podendo ser utilizada para a transmissão de outros tipos de sinais. Este tema é abordado na referência [14]. No entanto, as taxas de transmissão obtidas são muito inferiores as usadas em comunicações ópticas. Esta característica justifica o uso da criptografia quântica para a troca de chaves, pois não é requerido uma alta taxa de transmissão para este fim.

Uma segunda abordagem para a troca de chaves por meio das propriedades da camada física é baseada na aleatoriedade do canal. Esta aleatoriedade em redes sem fio é única para o transmissor e receptor. Esta técnica foi inicialmente investigada nas referências [15] e [16]. Atualmente este assunto continua sendo investigado, como, por exemplo, na referência [17]. Tradicionalmente esta técnica é mais estudada para redes sem fio, porém existe ao menos um trabalho [18] que aplica esta técnica em redes ópticas.

O último método de troca de chaves que será abordado nesta dissertação é a utilização de interferometria em redes ópticas. Foi publicado e demonstrado experimentalmente em [19] uma proposta em que a geração e o compartilhamento de chaves foram realizadas a partir da flutuação de fases do sinal transmitido na fibra. Na referência [20], esta técnica foi testada em um enlace de fibra monomodo padrão de 25 km.

1.2.3 Criptografia de sinais

Na criptografia de sinais, um sinal de entrada digital é convertido em um sinal criptografado analógico. Neste processo, o sinal é submetido às funções em que características do próprio sinal são parte das variáveis, junto às informações adicionais chaves. Nesta subseção abordaremos inicialmente os métodos atualmente pesquisados para criptografia de sinais modulados e de sinais em banda base. Em seguida, serão apresentados de quais maneiras a geração de chaves vem sendo realizada pelos diferentes trabalhos referenciados nesta seção.

1.2.3.1 Criptografia de sinais modulados

Existem várias técnicas propostas para a criptografia de sinais modulados. Uma delas é a criptografia caótica analógica. Esta técnica pode ser aplicada em comunicação sem fio ou em comunicação óptica. Nesta técnica, dois sistemas caóticos, um no transmissor e outro no receptor, são sincronizados mediante a transmissão de um sinal. Esta sincronização apresenta certo grau de dificuldade, porém soluções foram propostas nas referências [21] e [22] e foram revistas na referência [23]. Este tema continua sendo intensivamente pesquisado, sendo dois estudos mais recentes apresentados nas referências [24] e [25].

Outro conjunto possível de técnicas, pesquisada principalmente para sistemas ópticos, faz uso de efeitos não lineares em dispositivos ou fibras ópticas. Trabalhos que exploram este conjunto de técnicas estão apresentados,

por exemplo, nas referências [26] ─ [28]. Embora esta técnica funcione bem na teoria e em experimentos de laboratório, existem alguns desafios para sua implementação prática. É necessário, por exemplo, que os sinais ópticos envolvidos estejam temporalmente sincronizados. Além disso, a eficiência do sistema pode ser prejudicada caso os estados de polarização desses sinais não estejam alinhados. Estes desafios precisam ser superados para que esta proposta se torne uma solução comercial viável.

Um terceiro método de criptografia de sinais modulados é por meio da codificação de fatias espectrais. Este método é pesquisado principalmente para aplicação em redes ópticas. Seu princípio de funcionamento consiste em dividir o espectro do sinal em várias fatias e alterar individualmente alguma de suas propriedades com base em uma chave. Este tema foi explorado em [29], em que o espectro do sinal foi dividido e fases foram adicionadas individualmente em cada fatia. O receptor, em posse dos valores de fases adicionadas, realiza a divisão do espectro e subtrai das fases de cada fatia o valor da chave correspondente, recuperando o sinal. Posteriormente em 2015 [30], foi apresentada uma proposta que além de alterar a fase de cada fatia, também acrescenta um atraso temporal. Uma terceira alternativa sobre este método de criptografia foi apresentada em 2019 nas referências [31] ─ [33]. Nestes trabalhos, os espectros de dois ou mais sinais são divididos em várias fatias. Estas fatias são trocadas entre os sinais de forma pseudoaleatória para posterior transmissão. A forma com que as fatias são trocadas entre os sinais constitui a chave criptográfica, que é utilizada para a recuperação dos sinais.

Apesar de interessante do ponto de vista teórico, a criptografia de sinais modulados depende do desenvolvimento de dispositivos que operem na frequência do sinal modulado. Portanto, este método de criptografia está sujeito a um custo maior e limitações específicas de cada *hardware*. A criptografia de sinais se torna mais simples quando implementada em banda base, uma vez que seu desenvolvimento pode ser feito com base em processamento digital de sinais (d*igital signal processing*, DSP). Esta característica implica em um custo menor de implementação e em uma maior flexibilidade comparada à criptografia de sinais modulados.

1.2.3.2 Criptografia de sinais em banda base

A criptografia de sinais em banda base pode ser classificada em duas principais classes. A primeira classe é relativa aos métodos aplicáveis a sinais que posteriormente vão operar em sistemas de portadora única. Exemplos desses sinais são *Binary Phase Shift Keying* (BPSK), *Quadrature phase-shift keying* (QPSK) ou *16 Quadrature Amplitude Modulation* (16 QAM). Vários métodos de criptografia desta classe já foram publicados. Por exemplo, foi apresentado em [34] um método aplicado à redes sem fio, em que a encriptação é realizada nas amostras da fase do sinal. Em redes ópticas, podem ser citados, por exemplo, os trabalhos apresentados em [35] e [8]. Nas referências [36] e [37], que também estão relacionadas à comunicações ópticas, são apresentadas propostas de métodos que utilizam o embaralhamento espectral.

A segunda classe de criptografia de sinais em banda base é relativa a métodos que atuam em sinais que vão operar em sistemas de comunicação de múltiplas portadoras, como, por exemplo, a multiplexação por divisão de frequências ortogonais (*Orthogonal Frequency Division Multiplexing*, OFDM). Trabalhos que abordam métodos de criptografia desta classe foram publicados em [38] ─ [42].

1.2.3.3 Métodos de geração de chaves para criptografia de sinais

Os métodos de criptografia de sinais discutidos anteriormente utilizam a criptografia de blocos. Para os processos de encriptação e desencriptação de cada bloco, as chaves criptográficas precisam ser diferentes, não sendo possível sua reutilização. Portanto, torna-se necessário definir um método para a geração das chaves de cada bloco. Duas estratégias vêm sendo utilizada para este fim. A primeira delas, faz o uso de criptografia caótica digital, que foi proposta por Matthews [4] e foi apresentada na Subseção 1.1 Esta estratégia vem sendo extensivamente utilizada na literatura, principalmente em redes ópticas passivas (*passive optical network*, PON) com o uso do OFDM. Os trabalhos apresentados em [38] ─ [42] são exemplos desta aplicação.

Outra estratégia observada na literatura é a de chaves dinâmicas binárias. Um exemplo de aplicação desta estratégia foi apresentado em [37], que foi desenvolvido com base na referência [43] de 2010. Seu princípio de funcionamento consiste na troca das chaves inicial e temporária entre o transmissor e o receptor. Estas chaves são utilizadas para gerar uma chave semente, que é aplicada junto a chave temporária em uma função de mão única. Este processo gera a primeira chave dinâmica, que é utilizada para a encriptação do primeiro bloco. As demais chaves dinâmicas são geradas novamente com o uso da função de mão única, junto a chave semente e a chave dinâmica utilizada no bloco anterior. Este procedimento garante que as chaves criptográficas serão sempre diferentes entre blocos.

1.3 Contribuições

As principais contribuições desta dissertação são:

1. Apresenta-se uma proposta de adaptação da rede de Feistel para criptografia de sinais;
2. Apresenta-se uma possível forma de adaptação do modo de operação *Counter* (CTR) para criptografia de sinais;
3. Integram-se as propostas dos itens 1 e 2, atingindo uma técnica de criptografia de sinais que permite a reutilização de chaves entre blocos.
4. Avalia-se de maneira quantitativa as características de difusão, confusão e segurança semântica da estratégia descrita nos itens anteriores.

No melhor de nosso conhecimento, as contribuições 1, 2 e 3 nunca foram propostas na literatura. Sua implementação foi realizada a partir de um código desenvolvido também nesta dissertação, em linguagem Matlab®. Este software foi incluído ao software KryptoSJ, que é utilizado em demais projetos de pesquisa do grupo o qual este trabalho está inserido. Além disso, no início do mestrado foram estudados métodos de criptografia de sinais relativos a embaralhamento espectral, que foram fundamentais para adquirir-se maiores conhecimentos

sobre a criptografia da camada física. Estes estudos geraram publicações convidadas em eventos internacionais [32] - [33].

1.4 Organização da dissertação

O restante desta dissertação está organizado da seguinte maneira. O Capítulo 2 aborda algoritmos de encriptação e o modo de operação CTR aplicados à criptografia de dados. Este capítulo descreve os mecanismos de funcionamento da rede de Feistel, que é uma técnica clássica amplamente utilizada em criptografia de dados. Também é apresentado o *Tiny Encryption Algorithm* (TEA), que é uma técnica de criptografia baseada em redes de Feistel. Por fim, é apresentado o modo de operação CTR e o que motiva sua implementação junto a algoritmos de encriptação. No Capítulo 3 são apresentadas as propostas desta dissertação, que é a adaptação da rede de Feistel junto ao modo de operação CTR para a criptografia de sinais. Neste mesmo capítulo estão apresentados os cenários das simulações realizadas para as diferentes avaliações da técnica proposta. No Capítulo 4 são apresentados resultados referentes desde as avaliações iniciais que direcionaram todo o restante do desenvolvimento da técnica, análises sobre a confidencialidade da informação, até a avaliação de desempenho da técnica para a transmissão do sinal em um canal com ruído. O Capítulo 5 apresenta as conclusões obtidas com este trabalho e faz sugestões de passos que podem ser necessários para que a técnica proposta venha a se tornar uma solução comercial.

2. Algoritmos de encriptação e Modo de operação CTR

2.1 Rede de Feistel

Uma estrutura bastante utilizada em algoritmos de criptografia é a rede de Feistel [44], conforme apresentado na Figura 2. Nesta estrutura a mensagem original, que é uma sequência de bits, é dividido em duas metades, chamadas respectivamente de L_0 e R_0. A metade da direita, R_0, é utilizada como entrada de uma função F. Esta função também utiliza como entrada uma chave, identificada como K_0. As operações realizadas por esta função podem ser escolhidas de acordo com as características desejadas do algoritmo em questão. O resultado desta função, que continua sendo uma sequência de bits, é submetido à operação lógica XOR com a metade esquerda da mensagem original, L_0, gerando o vetor L_1 e finalizando o primeiro ciclo da rede de Feistel. No segundo ciclo, o vetor L_1 deve passar pelo mesmo processo descrito para o vetor R_0. O vetor R_0 deve ser submetido ao mesmo processo descrito para o vetor L_0.

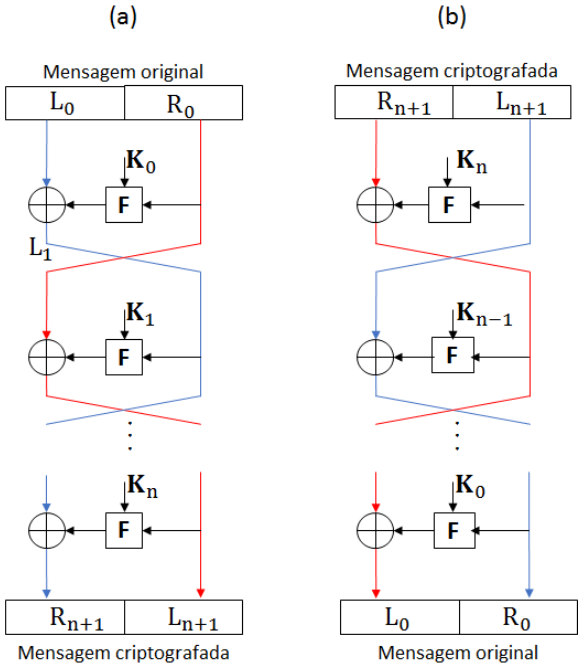

Figura 2 - (a) Processo de encriptação de um bloco. (b) Processo de desencriptação de um bloco

Os ciclos podem ser repetidos sucessivamente e novos vetores chaves podem ser utilizados. A quantidade de ciclos utilizados e a variedade das chaves aplicadas deve ser suficiente para promover as características de difusão, confusão e segurança semântica no sinal encriptado.

No processo de desencriptação são realizadas as mesmas operações, porém, com as chaves aplicadas em ordem inversa. A chave K_n deve ser a utilizada no primeiro ciclo de desencriptação. A chave K_1 deve ser a utilizada no último ciclo de desencriptação.

Um dos aspectos positivos da rede de Feistel é que qualquer que seja a função F utilizada, ela se tornará inversível. Isso possibilita a recuperação da mensagem no processo de desencriptação. Outro aspecto é que este é um algoritmo de criptografia de blocos. Isto permite que processos de encriptação e desencriptação ocorram de forma paralela, o que pode representar uma vantagem na agilidade do processamento de dados.

A rede de Feistel é utilizada em diversas técnicas comerciais de criptografia de dados [44] tais como o *Data Encryption Standard* (DES), o *Rivest Cipher 5* (RC5) e o TEA. O assunto da próxima seção é justamente o TEA.

2.2 Tiny Encryption Algorithm (TEA)

O TEA [45] é um algoritmo de criptografia baseado em Rede de Feistel. Este algoritmo, que está ilustrado na Figura 3, realiza a combinação de muitas funções de pouca complexidade. Este método promove boa segurança, performance razoável e fácil implementação comparado aos algoritmos que utilizam um menor número de funções de maior complexidade.

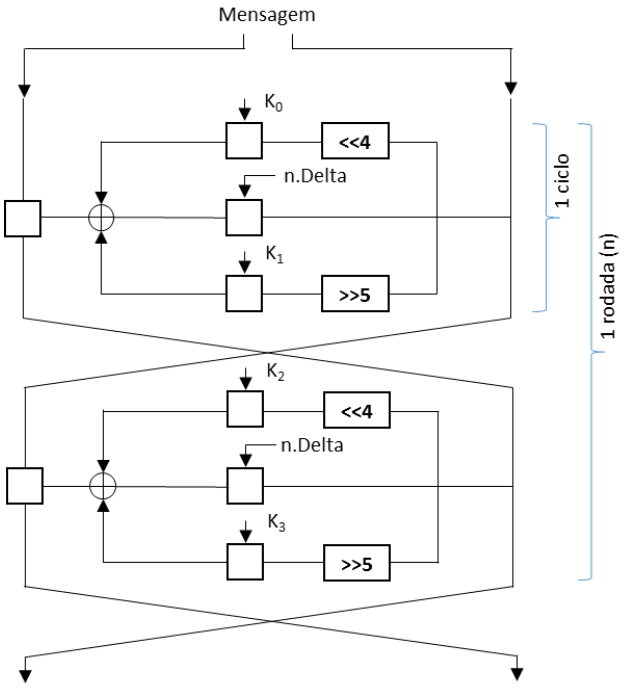

Figura 3 - Tiny Encryption Algorithm (TEA)

As informações de entrada deste algoritmo são: Mensagens de 32 bits de comprimento, 128 bits de informação chave, que são divididos em subchaves de 32 bits (K_0, K_1, K_2 e K_3) e a constante Delta. Esta constante é uma derivação do número de ouro, que é convertido para o formato binário, originando uma sequência de 32 bits. Porém, seus criadores identificaram que o desempenho do algoritmo não tem grande dependência desta constante. A utilização de outro valor, com a premissa de ser um número ímpar para uma aproximação de zero casas decimais, promoveria o mesmo desempenho [45].

No primeiro ciclo, a mensagem de entrada, que é a informação inicial, é dividida em duas metades. A metade da direita é submetida à três operações simultâneas. Na primeira, é realizado um deslocamento vetorial de 4 posições para a esquerda seguido da soma com a chave K_0. Na segunda operação, é realizada a soma de bits da mensagem com a sequência de bits da constante Delta. Na terceira, é realizado um deslocamento vetorial de 5 posições para a direita seguido da soma com a chave K_1. As sequências de bits resultantes destas três operações são submetidas à operação XOR. O resultado desta

operação é submetido à uma soma de bits com a metade esquerda da mensagem de entrada.

No segundo ciclo, a sequência de bits resultante da última operação descrita no parágrafo anterior é submetida as mesmas operações descritas para a metade direita da mensagem inicial. A metade direita da mensagem original é submetido as mesmas operações descritas para a metade esquerda da mensagem original. Porém, as chaves K_0 e K_1 são substituídas pelas chaves K_2 e K_3, respectivamente.

Para cada rodada subsequente do algoritmo são utilizadas as mesmas 4 chaves iniciais. A constante Delta se altera em valores proporcionais, conforme o número da rodada atual. Para criptografia de dados, observa-se o atendimento dos conceitos de difusão e confusão com 6 rodadas, ou seja, 12 ciclos. Desta forma, entende-se que seu desempenho também é satisfatório com a aplicação de 16 rodadas, que é a quantidade de rodadas utilizada no algoritmo de encriptação amplamente utilizado DES [46]. Os autores que criaram a técnica recomendam a utilização de 32 rodadas, que embora seja uma quantidade de rodadas maior que a utilizada no DES, se mostrou três vezes mais rápido em uma implementação de software [45].

2.3 Modo de Operação *Counter* (CTR)

Modos de Operação são utilizados junto a algoritmos de encriptação para a busca da confidencialidade da informação. Mas especificamente, um modo de operação é utilizado para garantir a segurança semântica do sistema. De acordo com o conceito *Perfect Secrecy* [47], uma mensagem encriptada não deve revelar nada sobre a mensagem não encriptada, mesmo que esta informação seja apenas se o transmissor está ou não dizendo algo. A utilização de um modo de operação pode permitir que mensagens e chaves idênticas gerem textos encriptados distintos. Portanto, atendendo o conceito de segurança semântica também é possível a reutilização de chaves para diferentes blocos encriptados.

Existem diferentes estruturas de modos de operação. Das possibilidades destas diferentes estruturas estão, por exemplo: A relação de dependência entre

blocos ou algoritmos independentes; a existência ou não de uma informação além da mensagem e da chave, normalmente chamada de vetor de inicialização; as formas de interação entre o vetor de inicialização, a mensagem, a chave e o texto encriptado em cada bloco.

Um dos modos de operação existentes é o CTR, que apresenta uma estrutura de criptografia de blocos independentes e utiliza um vetor de inicialização [48]. Este modo de operação está ilustrado na Figura 4. O vetor de inicialização e, não a mensagem, é submetido as principais operações do algoritmo. Inicialmente, este vetor é dividido em duas metades. A primeira metade, chamada *Nonce*, é definida como uma sequência de bits aleatório. A segunda metade, chamada *Counter*, é uma sequência de bits que opera como um contador binário, que muda de valor a cada bloco encriptado.

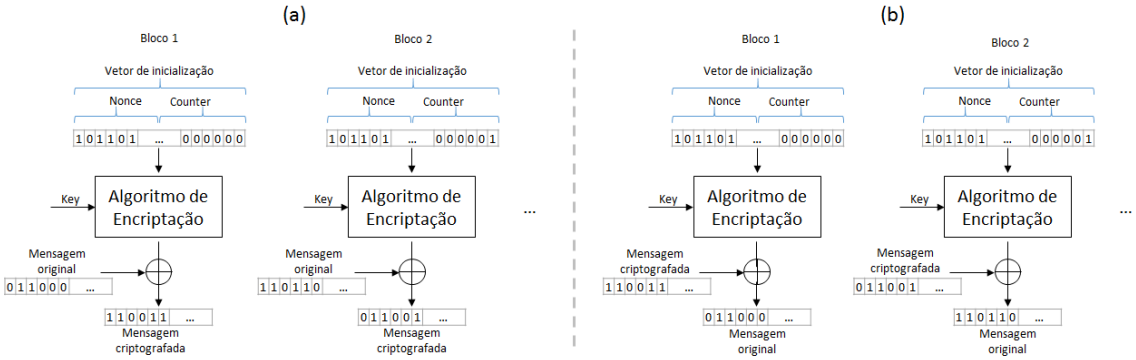

Figura 4 - Modo de Operação CTR. (a) Processo de encriptação. (b) Processo de desencriptação.

O vetor de inicialização é submetido ao Algoritmo de Encriptação, que pode ser uma das técnicas já apresentadas nas sessões anteriores. O resultado obtido é submetido à operação XOR com a mensagem. O resultado desta operação é o texto encriptado.

No algoritmo de desencriptação são realizadas as mesmas operações do algoritmo de encriptação, com exceção da operação XOR. Esta operação é

realizada com o texto encriptado recebido, e seu resultado é a mensagem descriptografada.

A utilização do Modo de Operação CTR permite maior flexibilidade no reuso de chaves, desde que o Algoritmo de Encriptação promova difusão. Desta forma, mesmo que o vetor de inicialização altere apenas um bit entre blocos, garante-se que aproximadamente 50% dos bits das mensagens encriptadas sejam diferentes entre blocos. Outra vantagem é que não existe dependência nas operações entre blocos, permitindo processamentos paralelos e o acesso aleatório da informação [49]. O algoritmo de desencriptação é o mesmo utilizado na encriptação, o que representa uma vantagem na simplicidade de implementação. Com isso, não são necessárias operações inversas [49]. Também é válido observar que a mensagem transmitida não é a informação que será submetida as principais operações do algoritmo de desencriptação, e sim o vetor de inicialização. Isso traz maior robustez ao sistema quanto a possíveis interferência na transmissão.

3. Proposta de algoritmo de encriptação

3.1 Descrição da técnica

Nesta proposta, foi desenvolvida uma técnica de criptografia de sinal análoga às metodologias já conhecidas para criptografia de dados. O modo de encriptação CTR foi adaptado junto à cifra de Feistel, permitindo a criptografia de blocos paralelos e independentes.

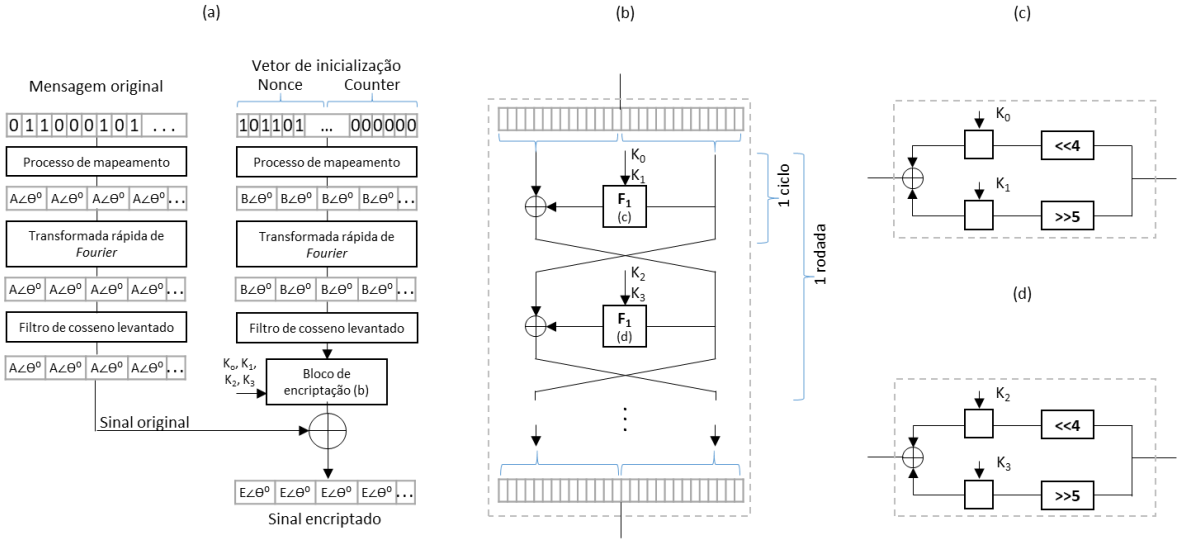

Figura 5 - Proposta de processo de encriptação. (a) Diagrama geral. (b) Detalhe do Bloco de encriptação. (c) Detalhe função F_1 com as chaves K_0 e K_1. (d) Detalhe função F_1 com as chaves K_2 e K_3.

Conforme ilustrado na Figura 5 (a), o vetor de inicialização funciona da mesma forma que na criptografia de dados. Os bits deste vetor são mapeados em uma sequência de símbolos, que são compostos por dois bits cada. Estas amostras, por representarem um sinal complexo no domínio do tempo, possuem uma amplitude e uma fase. Este sinal é submetido a um algoritmo de transformada rápida de Fourier, gerando o sinal no domínio da frequência. Este sinal passa por um filtro de cosseno levantado, que tem dupla função: limitar a largura de banda do sinal e nivelar a amplitude das componentes do espectro. O resultado desta operação é um novo vetor de amplitudes e fases. Este resultado

é utilizado como vetor de informação inicial no Bloco de Encriptação, que é uma cifra de Feistel e está detalhada na Figura 5 (b).

No primeiro ciclo da cifra de Feistel, o vetor de informação inicial é dividido em duas metades que chamaremos de metade direita e metade esquerda. A metade direita é submetida a uma função, F_1. Esta função, que está ilustrada nas Figuras 5 (c) e (d), foi desenvolvida com base no TEA, porém com algumas adaptações. Dois processos ocorrem de forma paralela. No primeiro, é aplicado um deslocamento vetorial de quatro posições de amostras para a esquerda, seguido de uma operação de adição com um vetor chave de fases aleatórias, chamado K_0. No segundo processo, é aplicado um deslocamento vetorial de cinco posições de amostras para a direita, seguido de uma operação de adição com um vetor chave de fases aleatórias, chamado K_1. Em seguida, é realizada a adição das fases dos vetores resultantes do primeiro e do segundo processos. As fases deste novo vetor são adicionadas às fases da metade esquerda do vetor de informação inicial, concluindo o primeiro ciclo da cifra de Feistel.

Para o segundo ciclo da cifra de Feistel torna-se necessária a criação de um novo vetor de informação inicial. A metade direita deste novo vetor é composta pelo resultado da operação descrita no parágrafo anterior. A metade esquerda deste novo vetor é composta pela metade direita do vetor de informação inicial original. Este novo vetor é submetido à função F_1 anteriormente descrita, porém substituindo-se os vetores chaves K_0 e K_1 por K_2 e K_3, respectivamente.

Nesta proposta, dois ciclos da cifra de Feistel são considerados uma rodada. Foram realizadas dez rodadas para a encriptação de cada bloco.

Na última etapa da encriptação, o sinal que contém a mensagem a ser transmitida é submetido a uma adição de fases no domínio da frequência com o vetor resultante do Bloco de encriptação. O resultado desta operação é o sinal encriptado, que será transmitido para o receptor

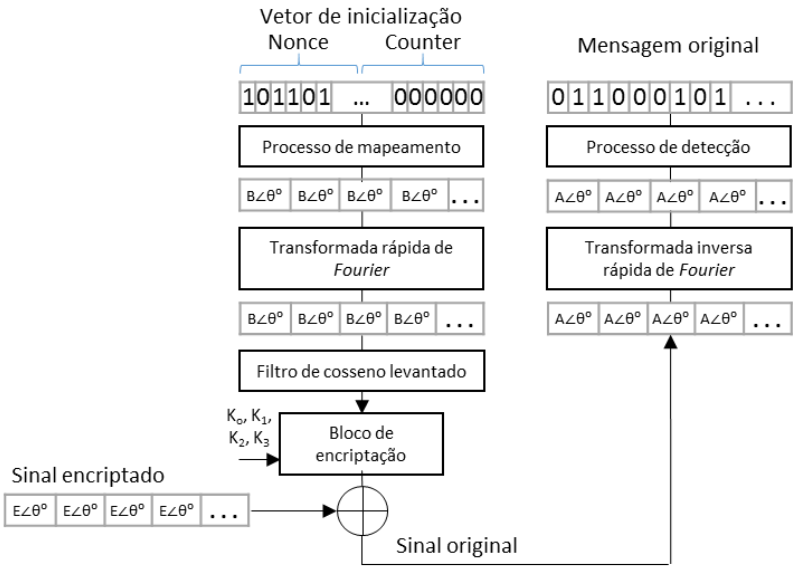

Figura 6 - Proposta de processo de desencriptação.

O algoritmo de desencriptação do sinal é semelhante ao de encriptação. Conforme ilustrado na Figura 6, implementa-se a mesma metodologia de geração do vetor de inicialização. Utilizam-se os mesmos vetores chaves e aplica-se a mesma cifra de Feistel do processo de encriptação. Entretanto, o texto cifrado recebido do transmissor deve ser submetido a uma subtração de fases, no domínio da frequência, com o vetor resultante do Bloco de Encriptação. O resultado desta operação é o sinal desencriptado no domínio da frequência, que submetido à transformada inversa rápida de *Fourier*, gera o sinal no domínio do tempo. Este sinal é submetido a um novo processo de mapeamento, em que as amplitudes e fases são substituídos por uma sequência de bits zeros e uns. Esta sequência de bits é a mesma da mensagem original.

O uso de um modo de operação, além de ser necessário para promover a segurança semântica do sistema, tem um objetivo especial para a criptografia de sinais, que é a robustez na recuperação de sinais sobre influência de ruído. Inicialmente, sem o uso do modo de operação, foram realizadas simulações de desempenho do algoritmo na recuperação de sinais com a ruído. Foi observado que a relação sinal-ruído (SNR) requerida para um valor de taxa de erro de bit (BER) próximo do limite da FEC estava muito alto. A mensagem somente pôde ser recuperada para valores de SNR na ordem de 200 dB, que é algo não usual

em um sistema de comunicação real. Perante este problema, foi necessário adotar um modo de operação. Foi observado que na estrutura de funcionamento do modo de operação CTR, no processo de recuperação da mensagem, o sinal recebido não é submetido ao algoritmo de desencriptação, mas sim, um sinal obtido a partir de um vetor de inicialização. Este vetor é gerado pelo próprio receptor e está livre das influências sofridas pelo sinal transmitido. Esta característica de funcionamento promove robustez ao processo de desencriptação, tornando possível a recuperação da mensagem para valores usuais de SNR. Os resultados obtidos que justificam esta escolha serão apresentados com maiores detalhes na seção 4.1.

3.2 Descrição das simulações

A técnica de encriptação proposta foi avaliada a partir de um código, de autoria própria, desenvolvido em linguagem Matlab®. O diagrama de blocos deste código está ilustrado na Figura 7. Foi utilizado como base para este desenvolvimento o código KryptosSJ [50], que foi desenvolvido pelo grupo de estudos que este trabalho está inserido. O software KryptoSJ em sua forma original está descrito no trabalho intitulado “Criptografia de Sinais Mediante Codificação Espectral Implantada por Meio de DSP e Aplicada a Redes Ópticas” [51]. O uso do modo de operação CTR foi realizado com base na dissertação de mestrado de Welerson Santos Souza, que está em desenvolvimento [52]. A BER foi estimada por meio de equações para o receptor ótimo de máxima verossimilhança na presença de um canal AWGN [53].

Para cada bloco encriptado, o vetor de inicialização é definido como uma sequência de x bits para o eixo I e x bits para o eixo Q, sendo x um número par. A metade destes bits em cada eixo, ou seja, $\frac{x}{2}$, são escolhidos de forma aleatória. Os outros $\frac{x}{2}$ bits são o contator binário que muda de valor a cada bloco encriptado.

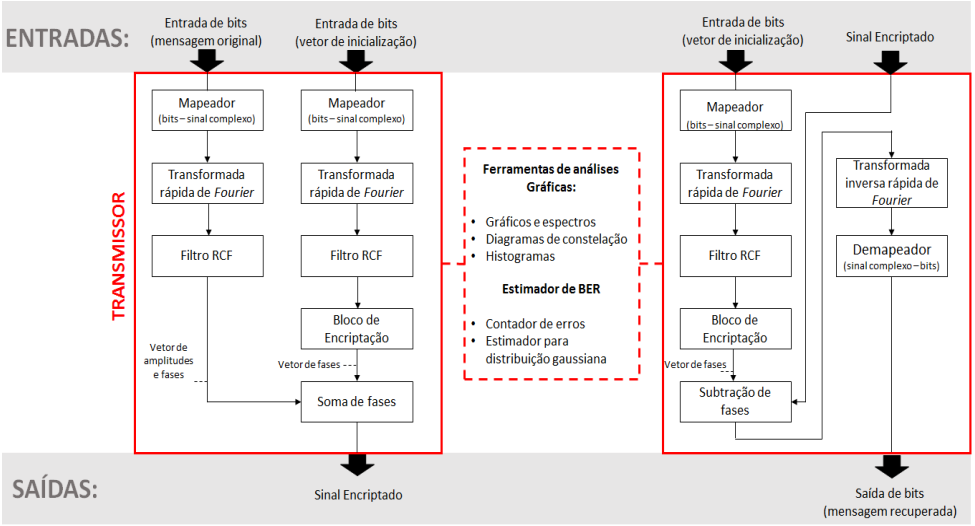

Figura 7 - Diagrama de blocos do código

Estes bits são mapeados em símbolos, sendo R_S a variável que representa a taxa de símbolo. Os símbolos representam um sinal equivalente complexo em banda base QPSK. Estas amostras são submetidas a um algoritmo de transformada rápida de *Fourier* (*Fast Fourier Transform*, FFT), dando origem a um sinal no domínio da frequência. Este sinal passa por um filtro de cosseno levantado (RCF), com fator de decaimento (*roll off*) de r. Este filtro: (i) nivela as amplitudes das componentes espectrais situadas entre $\frac{-R_S}{2} \cdot (1-r)$ e $\frac{R_S}{2} \cdot (1-r)$, (ii) atenua as componentes espectrais situadas entre $\frac{-R_S}{2} \cdot (1+r)$ e $\frac{-R_S}{2} \cdot (1-r)$ e $\frac{R_S}{2} \cdot (1-r)$ e $\frac{R_S}{2} \cdot (1+r)$ e (iii) elimina as componentes espectrais nas demais frequências. Na saída deste filtro, a quantidade de componentes mantidas é de $\frac{x}{2} \cdot (1+r)$. Estas componentes são amostras espectrais não nulas, de números complexos, que é a informação de entrada no Bloco de Encriptação

O Bloco de Encriptação realiza a encriptação do sinal, resultando em um novo conjunto de $\frac{x}{2} \cdot (1+r)$ amostras. Cada uma destas amostras é um número complexo, o qual apenas a fase será utilizada, conforme próximas etapas.

A mensagem original também é representada por uma sequência de x bits para o eixo I e x bits para o eixo Q. Estes bits também são mapeados em símbolos, que representam um sinal equivalente complexo em banda base. Da mesma forma, estas amostras passam por um algoritmo de transformada rápida

de *Fourier* e por um filtro RCF. Este resultado, que é um conjunto de $\frac{x}{2} \cdot (1 + r)$ amostras de números complexos, que tem suas fases somadas as fases do conjunto de amostras gerado pelo Bloco de Encriptação. O resultado, que é um novo vetor de números complexos, é o sinal encriptado no domínio da frequência.

As simulações foram realizadas para sistema *back to back* (B2B), em que o transmissor está conectado diretamente ao receptor. Também foram realizadas simulações considerando um canal com ruído aditivo branco e gaussiano (*Additive White Gaussian Noise*, AWGN). As chaves criptográficas são vetores de $\frac{x}{2} \cdot (1 + r)$ posições. Cada posição deste vetor é um valor aleatório de -π a π, podendo ser gerado com uma determinada quantidade de bits de resolução.

Neste capítulo foi apresentado o funcionamento da técnica de criptografia de sinais proposta neste trabalho. Também foi apresentado o cenário das simulações para a avaliação da técnica. No próximo capítulo, serão apresentadas as avaliações realizadas sobre a técnica, junto aos resultados obtidos.

4. Resultados

Este capítulo aborda os resultados referentes as simulações da técnica proposta no Capítulo 3. Todos resultados foram obtidos a partir de simulações computacionais. Foram realizadas análises para configuração B2B, em que o transmissor está conectado diretamente ao receptor. Também foram realizadas análises verificando o desempenho do sistema com um canal AWGN. A mensagem e o vetor de inicialização foram encriptados em blocos de 116 bits que resultaram, após o filtro RCF, em 64 amostras espectrais de sinais não nulas.

O restante deste capítulo está organizado da seguinte forma. Na Seção 4.1 será apresentada a análise para definição da quantidade de rodadas na rede de Feistel, na Seção 4.2 será apresentado o desempenho da técnica sem o uso do modo de operação CTR, na Seção 4.3 será verificado o desempenho da proposta completa de criptografia de sinais, que é o objeto deste trabalho.

4.1 Análise para a definição da quantidade de rodadas na rede de Feistel

Para que as redes de Feistel ofereçam (i) BER da mensagem encriptada adequada, (ii) difusão e (iii) confusão, é necessário um certo número mínimo de rodadas. Por esta razão, nesta seção foi analisado qual é este número mínimo. Os requisitos estabelecidos para estas três características são: BER da mensagem encriptada com valor aproximado de 0,5; a difusão com valor aproximado de 50%; a confusão com valor aproximado de 50%. O atendimento destes requisitos é analisado especificamente sobre o Bloco de Encriptação, conforme Figura 8 (a). O modo de operação não é considerado nesta avaliação. Esta simulação foi repetida para diferentes quantidades de rodadas na rede de Feistel, sendo a informação de entrada a palavra A e a informação encriptada a palavra B, conforme Figura 8 (b). Inicialmente, a simulação foi realizada para uma rodada, verificando-se o comportamento das três características citadas. Em seguida foram acrescentadas rodadas até que o algoritmo promovesse o atendimento dos três requisitos estabelecidos.

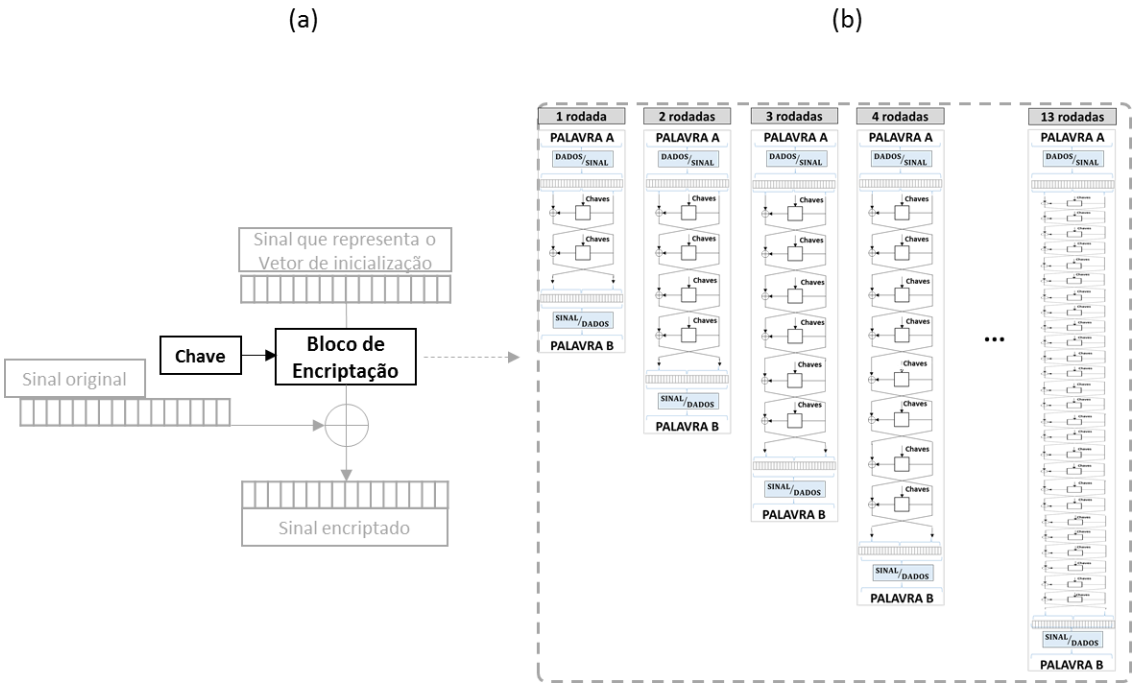

Figura 8 - Rede de Feistel com diferentes quantidades de rodadas

O primeiro requisito observado foi a BER da mensagem encriptada. O resultado desta análise está exposto na Figura 9. Valores de BER acima do limite estabelecido de $2 \cdot 10^{-3}$ conforme linha vermelha do gráfico, demonstram que intrusos terão uma grande dificuldade para recuperar a mensagem, mesmo com o uso de FEC na recepção do sinal. Observou-se que a BER da mensagem encriptada atingiu valor aproximado de 0,5 com apenas uma rodada na rede de Feistel. Este é o valor desejado para uma mensagem encriptada, pois representa o valor máximo de encriptação da mensagem. Não foram observadas grandes variações para maiores quantidades de rodadas.

Para a análise da difusão, os bits que geram a chave de fases e os bits da mensagem original foram fixados. A mensagem e a chave foram submetidas ao Bloco de Encriptação, que originou uma mensagem encriptada. Esta mensagem encriptada foi definida como referência para futuras comparações. Para cada bloco subsequente encriptado, alterou-se apenas um bit na mensagem original de referência, mantendo a informação da chave sempre a mesma. A quantidade de bits alterados na mensagem encriptada de cada bloco, comparada à mensagem encriptada de referência, foi a forma escolhida para quantificar a difusão da rede de Feistel.

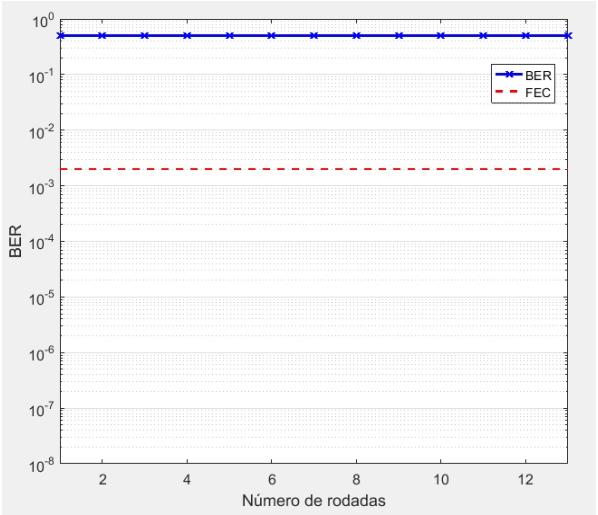

Figura 9 - Análise da BER da mensagem encriptada em função do número de rodadas da rede de Feistel

O gráfico da Figura 10 apresenta o comportamento da difusão em função do número de rodadas utilizadas na rede de Feistel. Observou-se que com uma rodada, cerca de 21% dos bits são diferentes entre os blocos. Ao acrescentar mais rodadas, observou-se uma tendência de aumento do número de bits diferentes entre blocos, sendo que para três ou mais rodadas este número aumentou para aproximadamente 50%. Este é o valor esperado para este requisito.

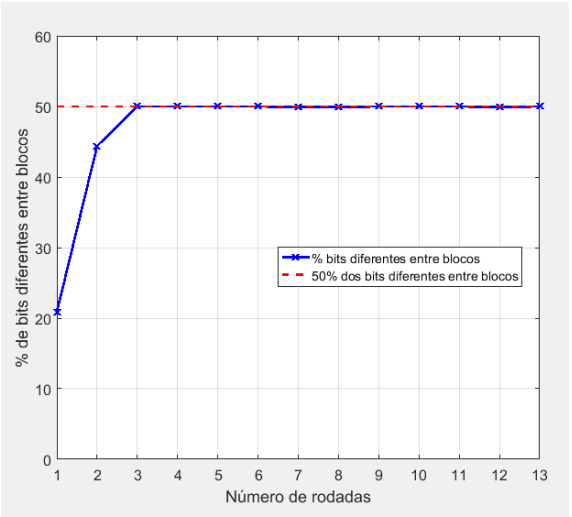

Figura 10 - Difusão provida pela rede de Feistel em função do número de rodadas

Para a análise da confusão foram fixados os bits que geram a chave de fases e os bits da mensagem original. Cada posição da chave, que variam de -π a π, é representada com uma resolução de 10 bits. A mensagem e a chave foram submetidas ao Bloco de Encriptação, gerando uma mensagem encriptada de referência. Nos blocos subsequentes, a mensagem original permaneceu a mesma, e a informação chave teve um bit alterado em cada bloco, comparado ao bloco inicial que gerou a mensagem encriptada de referência. A quantidade de bits alterados na mensagem encriptada de cada bloco, comparada à mensagem encriptada de referência, foi a forma adotada para quantificar a confusão da rede de Feistel. É possível observar na Figura 11 que com a utilização de 11 rodadas a quantidade de bits diferentes da mensagem encriptada entre blocos foi de aproximadamente 50%, que é o valor estabelecido para o atendimento deste requisito.

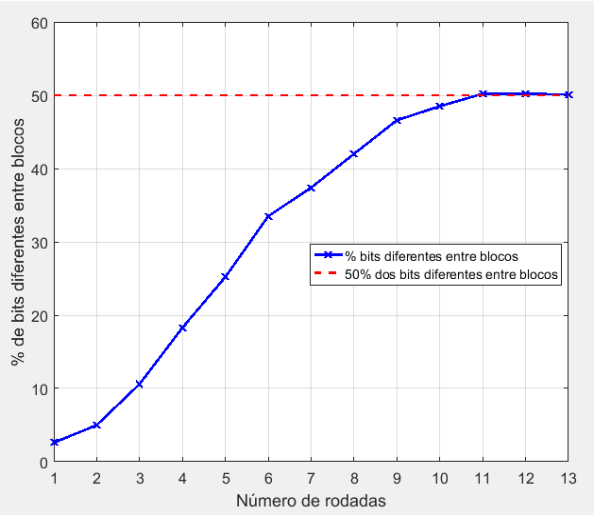

Figura 11 - Confusão provida pela rede de Feistel em função do número de rodadas

Analisando as Figuras 10 e 11, verifica-se que foi necessário um maior número de rodadas para atingir o requisito da confusão, comparada à quantidade de rodadas necessárias para atingir o requisito da difusão. O motivo desta necessidade é que, devido aos valores de chave terem uma resolução de 10 bits, a alteração de um bit entre blocos pode representar uma alteração muito

pequena na chave. Considerando a situação mais crítica sobre este aspecto, em que apenas o bit menos significativo mude de valor entre blocos, isso representaria a alteração de apenas 0,0061 radianos em uma das posições da chave. Com a possibilidade de uma alteração tão pequena na chave entre blocos, é justificado um maior número de rodadas para que a mensagem encriptada seja afetada o suficiente.

Observado que com 11 rodadas as três características analisadas tiveram resultados satisfatórios, definiu-se como 11 a quantidade de rodadas padrão para a técnica proposta.

4.2 Desempenho sem o modo de operação CT

Após a definição da quantidade de rodadas necessárias, foi verificado o desempenho do Bloco de Encriptação, sem a utilização uso do modo de operação, para a situação B2B, modulação QPSK e taxa de símbolo de 10 GBaud. Conforme apresentado na Figura 12, a constelação e o histograma dos sinais original e desencriptado são semelhantes. A BER da mensagem desencriptada foi igual a zero, indicando que o sinal recuperado não possui erros. A constelação do sinal encriptado apresenta pontos aleatoriamente distribuídos em formato circular. Os histogramas dos dados dos eixos real e imaginário apresentam distribuições gaussianas, centralizadas em zero. A BER da mensagem encriptada foi aproximadamente 0,5, que é o resultado desejado para uma mensagem encriptada.

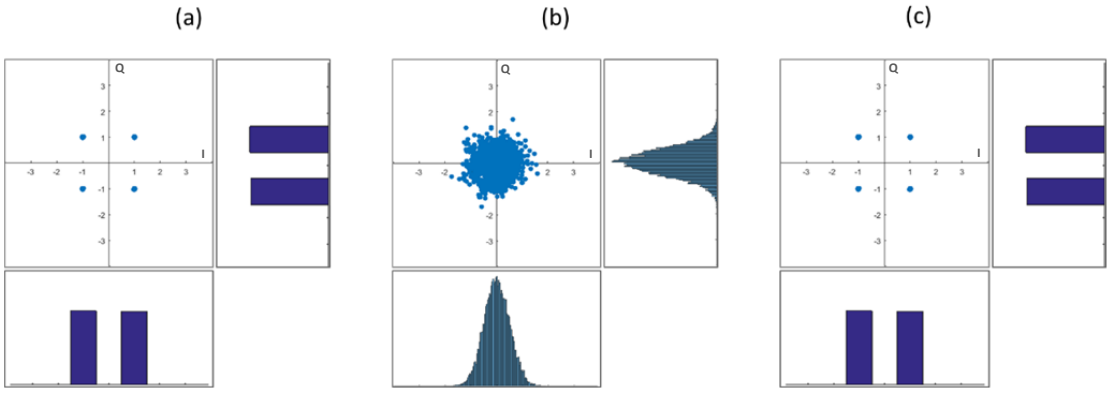

Figura 12 - Situação B2B, constelação e histogramas dos dados dos eixos real e imaginário (a) Sinal original (b) Sinal encriptado (c) Sinal desencriptado

A próxima avaliação realizada sobre o Bloco de Encriptação, sem a utilização do modo de operação, foi verificar o seu desempenho com a transmissão do sinal encriptado por um canal AWGN, modulação QPSK e taxa de símbolo de 10 GBaud. Inicialmente, foi realizada a simulação com valor de SNR de aproximadamente 13 dB e foram analisados as constelações e os histogramas dos sinais original, encriptado e desencriptado. A partir desta análise, é possível observar na Figura 13 que as constelações e os histogramas dos sinais encriptado e desencriptado são semelhantes. A BER obtida para ambos sinais foi de aproximadamente 0,5, demonstrando a incapacidade do algoritmo recuperar a mensagem com este valor de SNR.

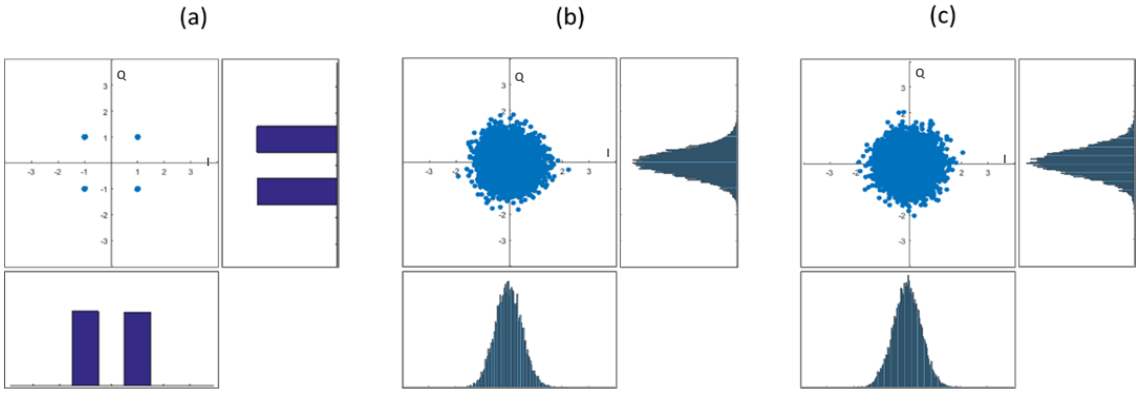

Figura 13 – Resultados em um canal AWGN com SNR de 13 dB, constelação e histogramas dos dados dos eixos real e imaginário (a) Sinal original (b) Sinal encriptado (c) Sinal desencriptado.

Novas simulações foram realizadas alterando-se a amplitude do ruído e, por consequência, o valor da SNR. Os resultados estão apresentados na Figura 14. Observou-se que para níveis usuais de SNR, a BER da mensagem desencriptada se manteve em aproximadamente 0,5. Estes valores estão acima do limite máximo estabelecido pelo FEC, indicado pela linha vermelha do gráfico. Estes valores não são desejáveis para uma mensagem após desencriptação.

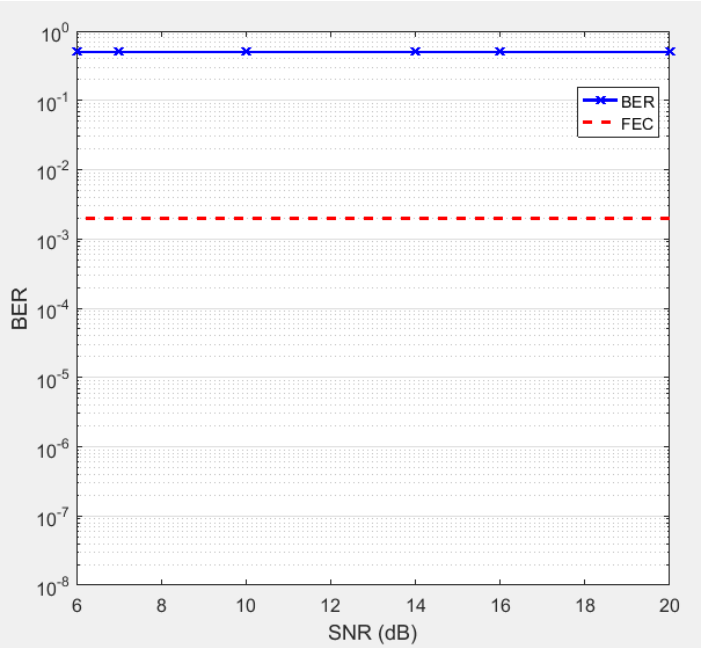

Figura 14 - BER da mensagem desencriptada em função da SNR sem o modo de operação CTR

Para determinar o valor da SNR no qual a BER atinge o limite da FEC, foram feitas simulações com valores crescentes de SNR. Verificou-se que a BER atinge o limite da FEC apenas para uma SNR da ordem de 200 dB. No entanto, este valor é muito elevado e dificilmente poderia ser obtido em um sistema real de comunicação.

Os resultados apresentados nesta seção demonstram a incapacidade do algoritmo recuperar o sinal encriptado com valores usuais de SNR. Isso ocorre porque o algoritmo de encriptação requer que o sinal recebido seja o mesmo que o sinal transmitido. No entanto, ao se propagar por um canal AWGN, o ruído faz com que o sinal recebido seja distinto do sinal transmitido, não permitindo que a descriptografia atue corretamente.

A utilização do modo de operação CTR foi identificada como uma solução possível para este problema. A principal justificativa para sua utilização, é que o sinal transmitido não é submetido às operações do algoritmo de desencriptação, mas sim, um sinal gerado pelo próprio receptor. Este sinal, que não foi modificado pelo ruído do canal, é obtido a partir de uma sequência de bits, chamado vetor de inicialização. Esta sequência é única para cada bloco encriptado. O desempenho da proposta utilizando este modo de operação será apresentado na seção seguinte.

4.3 Desempenho da técnica

Nesta seção serão apresentadas as análises de desempenho e os resultados obtidos sobre a solução proposta completa, que é a junção do Bloco de Encriptação com o modo de operação CTR. Esta solução está apresentada nas Figuras 5 e 6 da Seção 3.1.

4.3.1 Análise para situação B2B e canal AWGN

Inicialmente, foi realizada a simulação para a situação B2B, com modulação QPSK e taxa de símbolo de 10 GBaud. Conforme apresentado na Figura 15, as constelações e os histogramas dos sinais original e desencriptado são semelhantes. A BER da mensagem desencriptada é zero, indicando que o sinal pôde ser recuperado sem penalidades. A constelação do sinal encriptado apresenta pontos distribuídos de forma difusa. Os histogramas dos dados dos eixos real e imaginário apresentam distribuições gaussianas centralizadas em zero. A BER da mensagem encriptada foi aproximadamente 0,5, que é o valor esperado de uma mensagem encriptada.

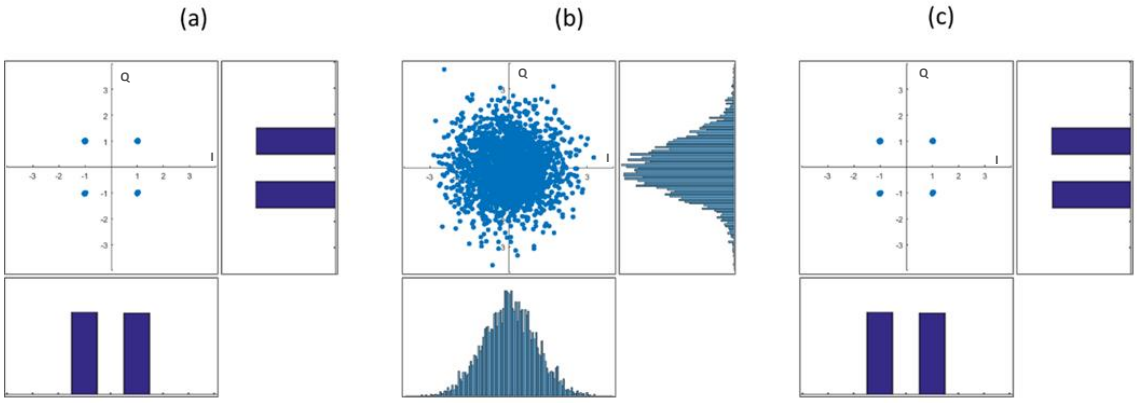

Figura 15 - Situação B2B, constelação e histogramas dos dados dos eixos real e imaginário (a) Sinal original (b) Sinal encriptado (c) Sinal desencriptado.

Em seguida, foi verificado o desempenho da técnica com a transmissão do sinal encriptado por um canal AWGN, modulação QPSK e taxa de símbolo de 10 GBaud. Novamente, foi realizada a simulação com valor de SNR próximo de 13 dB e foram analisadas as constelações e os histogramas dos sinais original, encriptado e desencriptado. É possível observar na Figura 16 que a constelação do sinal desencriptado apresenta uma leve alteração comparada a constelação do sinal original. Esta alteração não impossibilita a recuperação da mensagem, visto que a BER, de $\approx 4{,}6 \cdot 10^{-4}$ está abaixo do limite da FEC.

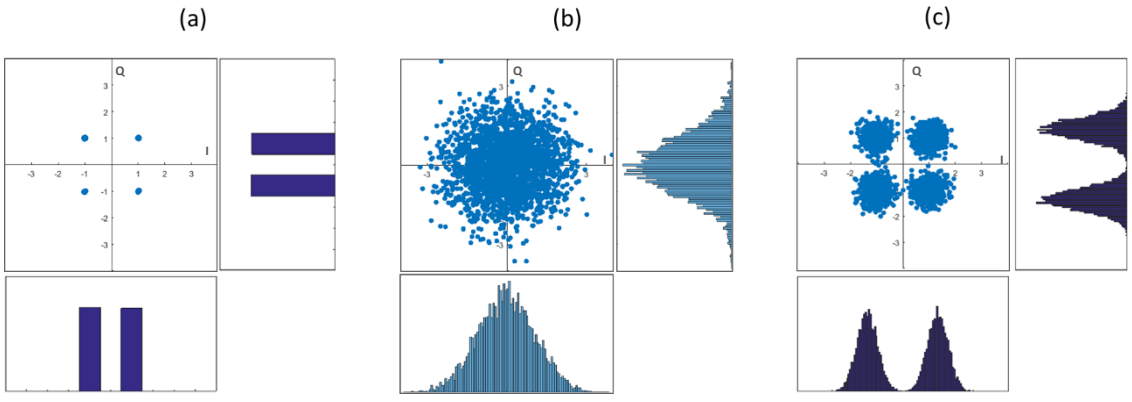

Figura 16 - Resultados em um canal AWGN com SNR de 13 dB, constelação e histogramas dos dados dos eixos real e imaginário (a) Sinal original (b) Sinal encriptado (c) Sinal desencriptado.

O cenário da última simulação descrita foi repetido para diferentes valores de SNR. As constelações obtidas e as respectivas BERs das mensagens desencriptadas estão apresentadas na Figura 17. É possível observar que a BER da mensagem desencriptada aumenta à medida que a SNR diminui. Da mesma forma, é possível observar como este comportamento reflete na constelação do sinal.

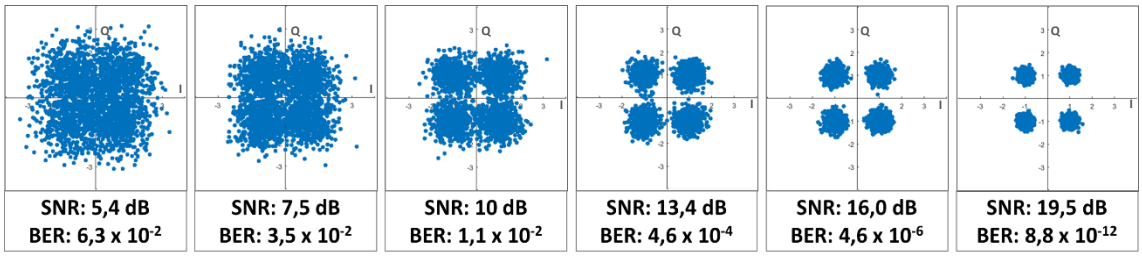

Figura 17 - Constelação do sinal desencriptado para diferentes valores de SNR

A próxima análise realizada foi a comparação do desempenho do algoritmo de desencriptação com um sistema sem qualquer algoritmo de encriptação. Esta análise está apresentada na Figura 18. Para ambos os casos, o sinal foi submetido a um canal AWGN, com modulação QPSK e taxa de símbolo de 10 GBaud.

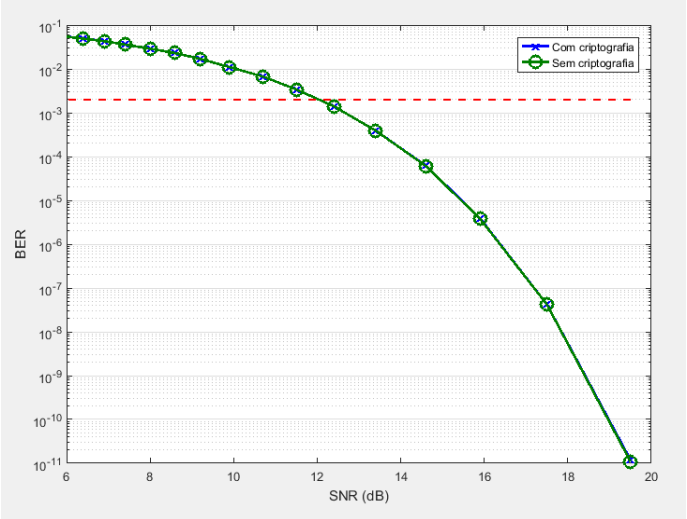

Figura 18 - BER em função da SNR com e sem criptografia

É possível observar que as curvas são próximas. Isso demonstra que a técnica de criptografia proposta não penaliza de forma significativa o sistema de comunicação. A equivalência de desempenho de um sistema com e sem a técnica de criptografia proposta foi alcançada devido ao uso do modo de operação CTR. Isso acontece pois neste modo de operação, o Bloco de Encriptação não atua sobre o sinal transmitido, mas sobre um sinal gerado pelo próprio receptor, que não foi submetido ao ruído do canal.

4.3.2 Confidencialidade: Difusão, confusão e segurança semântica

A análise da difusão foi realizada da mesma forma descrita para a escolha da quantidade de rodadas na rede de Feistel. Esta análise é realizada especificamente no Bloco de Encriptação, sem considerar o modo de operação. A simulação foi repetida 13 mil vezes, de forma a obter uma quantidade representativa de amostras. Estas amostras foram analisadas em um histograma e está apresentado na Figura 19. O formato observado é aproximadamente o de uma gaussiana, com valor médio da quantidade de bits alterados na mensagem encriptada em relação ao número total de bits de 50,1%. O desvio padrão é de 4,9%.

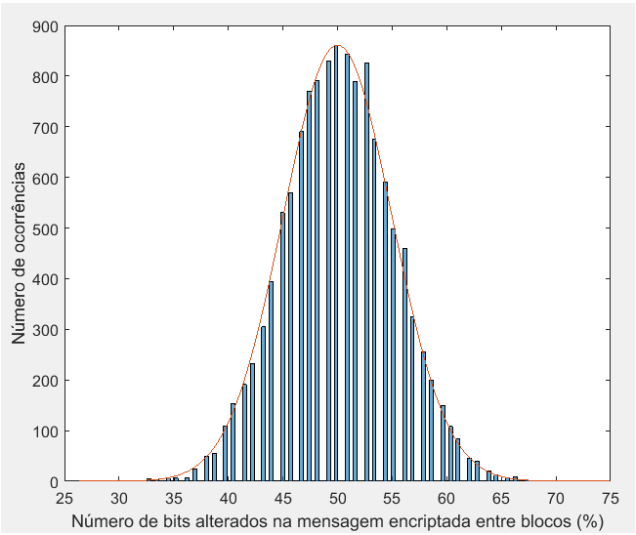

Figura 19 - Análise da difusão do algoritmo.

A forma de analisar a confusão foi a mesma descrita para a escolha da quantidade de rodadas na rede de Feistel. O resultado desta análise está apresentado na Figura 20. A simulação foi repetida 13 mil vezes para obter-se um número representativo de amostras no histograma, que apresentou a forma de uma gaussiana. O valor médio da quantidade de bits alterados na mensagem encriptada em relação ao número total de bits de 50,1%. O desvio padrão foi de 5,3%

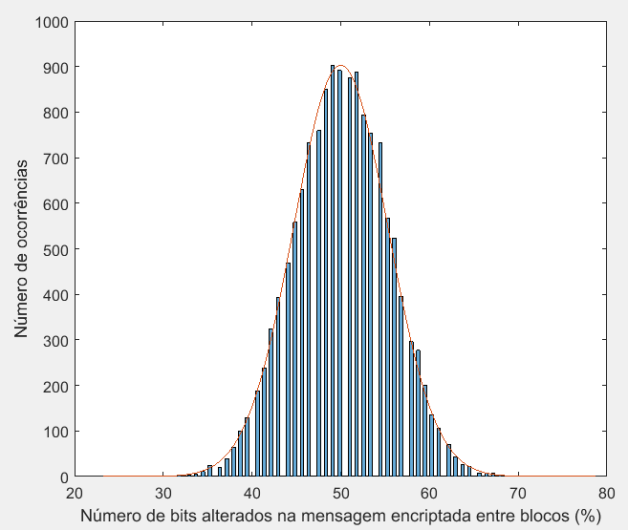

Figura 20 - Análise da confusão do algoritmo.

A análise da segurança semântica é realizada sobre todo o algoritmo de encriptação. Para que um algoritmo de encriptação promova segurança semântica, é necessário que blocos encriptados com mensagens e chaves iguais produzam mensagens encriptadas diferentes. Para esta análise, os bits da mensagem original e os valores de chave se mantiveram os mesmos. A única informação alterada em cada bloco foi a sequência de bits do vetor de inicialização correspondente ao *Counter*. A representação gráfica da análise da segurança semântica esta apresentada na Figura 21. Em cada ponto deste gráfico, a coordenada z indica a quantidade de bits iguais ao comparar-se os bits do bloco indicado pela coordenada x com os bits do bloco indicado pela coordenada y. Foram encriptados 250 blocos para esta análise. É possível observar que a taxa de bits iguais nas mensagens encriptadas entre blocos está

em torno de 50%, com exceção do caso em que a comparação é feita o bloco e ele próprio. Nesta situação a taxa é 100%, conforme esperado

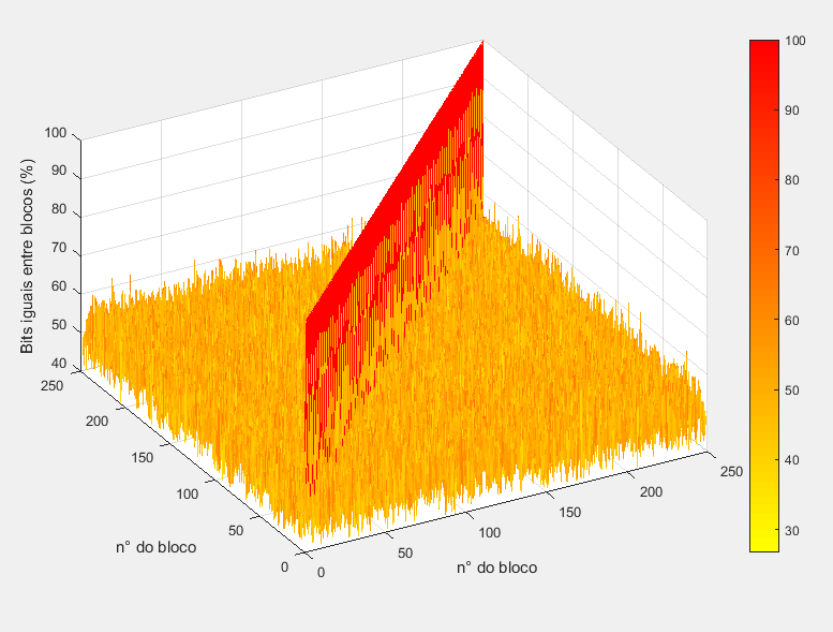

Figura 21 - Análise da segurança semântica do algoritmo.

Os resultados apresentados neste capítulo demonstram desempenho satisfatório para os cenários simulados. Dentro das características de segurança avaliadas, a proposta se mostrou bem sucedida, sendo, portanto, promissora para utilização em sistemas práticos.

5. Conclusão

Neste trabalho, propôs-se uma estratégia para adaptar o uso de redes de Feistel à criptografia de sinais. Nesta adaptação, a informação de entrada foi dividida em blocos de 116 bits, que passaram por um processo de mapeamento e conversão, gerando um sinal no domínio da frequência de 64 amostras não nulas. Este sinal é submetido ao Bloco de Encriptação, que é composto por rodadas da rede de Feistel, com funções inspiradas no padrão TEA. Observou-se na mensagem encriptada que, com apenas uma rodada, a BER foi de 0,5. Com a utilização de 3 ou mais rodadas, a difusão foi atingida. A confusão foi alcançada com 11 rodadas, que motivou tornar este o número de rodadas padrão da rede de Feistel. Sendo assim, o Bloco de Encriptação apresenta desempenho satisfatório em relação a BER, a difusão e a confusão. No entanto, apenas a utilização do Bloco de Encriptação não promove a segurança semântica. Adicionalmente, o desempenho foi insatisfatório quando ocorre a presença de ruído. Ambos estes problemas foram resolvidos a partir da proposta de uma estratégia que adapta o modo de operação CTR à criptografia de sinais

A segurança semântica, que estabelece que a mensagem encriptada não deve revelar nada da mensagem original, foi avaliada encriptando-se vários blocos com mensagens e chaves iguais, esperando-se mensagens encriptadas diferentes. Esta condição foi simulada e os resultados demonstram que o modo de operação CTR, adaptado à criptografia de sinais, junto ao Bloco de Encriptação, adaptado à criptografia de sinais, proporciona segurança semântica. A técnica de criptografia proposta também possibilitou que o sinal encriptado transmitido por um canal com ruído, pudesse ser recuperado de forma satisfatória. Nesta análise, o sinal encriptado pôde ser recuperado sem penalidades significativas quando comparado a um sinal transmitido e recebido sem nenhum método de encriptação operante.

Outro aspecto importante proporcionado pelo uso do modo de operação CTR, é a possibilidade de reutilização de chaves para vários Blocos de Encriptação. A rede de Feistel é aplicada sobre o sinal gerado pelo vetor de inicialização, que sempre será diferente entre blocos. Desta forma, mesmo que a chave se mantenha a mesma, o sinal de saída do Bloco de Encriptação será

diferente entre blocos. Isto ocorre devido ao Bloco de Encriptação atender ao requisito da difusão. O reuso de chaves para criptografia de sinais é uma característica que, no melhor de nosso conhecimento, ainda não foi proposta na literatura.

Conclui-se, para as condições simuladas, que a técnica proposta nesta dissertação é uma solução promissora para promover a confidencialidade de sinais. Observou-se que os requisitos de BER, difusão, confusão e segurança semântica foram atendidos, a partir da proposta de soluções inéditas, no melhor de nosso conhecimento, na literatura. Com isso, entende-se que esta proposta deve continuar sendo pesquisada, verificando seu desempenho com outros sinais equivalentes complexos como BPSK e 16-QAM e com diferentes taxas de símbolos. Recomenda-se que sejam realizadas simulações de transmissão do sinal por fibra óptica por meio de softwares específicos como, por exemplo, o VPI®. Em um próximo passo, esta técnica poderia ser implementada em um hardware através de uma plataforma programável como, por exemplo, um FPGA (*Field Programmable Gate Array*, FPGA) ou um chip específico. Com isso, testes de campo poderiam ser realizados de forma que, no futuro, esta técnica esteja mais próxima de ser uma solução comercial para a confidencialidade da informação aplicada na camada física.

Lista de publicações

1. Santos, M. de O.; Souza, W. S.; Bragagnolle, T. de A.; Bobadilla, L. D. B.; Aldaya, I.; Prado, A. J. do; Ferreira, A. A.; Bonani, L. H.; Abbade, M. L. F. All-optical Spectral Shuffling Applied to 16-QAM Signals. 2019 SBFoton International Optics and Photonics Conference (SBFoton IOPC), 2019

2. Bragagnolle, T. de A.; Pereira Nogueira, M.; de Oliveira Santos, M.; do Prado, A. J.; Ferreira, A. A.; de Mello Fagotto, E. A.; Aldaya, I.; Abbade, M. L. F. All-optical spectral shuffling of signals traveling through different optical routes. In: 2019 21st International Conference on Transparent Optical Networks (ICTON). [S.l.:s.n.], 2019. p.1-4. Trabalho convidado.

Referências

[1] STALLINGS, William. “Cryptography and Network Security: Principles and Practices,” Fourth Edition. ed. [S. l.]: Prentice Hall, 2005. 592 p. Citado 4 vezes na página 12.

[2] KATZ, Jonathan; YEHUDA, Lindell J. Katz and Y. Lindell, “Introduction to modern cryptography,” CRC press, 2014. Citado 1 vez na página 14.

[3] PFLEEGER, C. P. “Security in Computing,” 4a edição. Prentice Hall, 23 de outubro de 2006 880pág. Citado 1 vez na página 14.

[4] R. Matthews, “On the derivation of a ‘chaotic’ encryption algorithm,” Cryptologia, vol. 13, no. 1, pp. 29–42, 1989.. Citado 2 vezes nas páginas 14 e 19.

[5] G. Alvarez and S. Li, “Some basic cryptographic requirements for chaos-based cryptosystems,” Int. J. Bifurc. Chaos, vol. 16, no. 8, pp. 2129–2151, 2006. Citado 2 vezes na página 15.

[6] J. Sen Teh, M. Alawida, and Y. C. Sii, “Implementation and practical problems of chaos-based cryptography revisited,” J. Inf. Secur. Appl., vol. 50, no. August 2019, 2020. Citado 3 vezes na página 15.

[7] Ben Wu,* Zhenxing Wang, Yue Tian, Mable P. Fok, Bhavin J. Shastri, Daniel R. Kanoff and Paul R. Prucnal, “Optical steganography based on amplified spontaneous emission noise,” Lightwave Communications Laboratory, Department of Electrical Engineering, Princeton University, Princeton, New Jersey 08544, USA. Citado 1 vez na página 15.

[8] E. Wohlgemuth, Y. Yoffe, T. Yeminy, Z. Zalevsky, and D. Sadot, “Demonstration of coherent stealthy and encrypted transmission for data center interconnection,” Opt. Express, vol. 26, no. 6, p. 7638, 2018. Citado 2 vezes nas páginas 15 e 19.

[9] C. H. Bennet and G. Brassard, “Quantum Cryptography: Public Key Distribution and Coin Tossing,” in International Conferecen on Computers, Systems & Signal Processing, 1984, pp. 175–179. Citado 1 vez na página 16.

[10] A. K. Ekert, “Physical Review Letters,” Phys. Rev. Lett., vol. 67, no. 5, pp. 661–663, 1991.Citado 1 vez na página 16.

[11] Y. Mao et al., “Integrating quantum key distribution with classical communications in backbone fiber network,” Opt. Express, vol. 26, no. 5, p. 6010, 2018. Citado 1 vez na página 16.

[12] ID Quantique, “Cerberis QKD System,” Product Brochure, pp. 1–4, 2018.Citado 1 vez na página 16.

[13] S. K. Liao et al., “Satellite-to-ground quantum key distribution,” Nature, vol. 549, no. 7670, pp. 43–47, 2017. Citado 1 vez na página 16.

[14] A. Broadbent and C. Schaffner, “Quantum cryptography beyond quantum key distribution,” vol. 78, no. 1. Springer US, 2016. Citado 1 vez na página 16.

[15] A. D. Wyner, “The Wire-Tap Channel,” Bell Syst. Tech. J., vol. 54, no. 8, pp. 1355–1387, Citado 1 vez na página 16.

[16] I. Csiszar and J. Korner, “Broadcast Channels,” Inf. Theory, vol. IT-24, no. 3, pp. 339–348, 1978. 1975. Citado 1 vez na página 16.

[17] H. Yu, T. Kim, and H. Jafarkhani, “Wireless Secure Communication with Beamforming and Jamming in Time-Varying Wiretap Channels,” IEEE Trans. Inf. Forensics Secur., vol. 13, no. 8, pp. 2087–2100, 2018. Citado 1 vez na página 16.

[18] V. Forutan, R. Elschner, C. Schmidt-langhorst, C. Schubert, and R. F. H. Fischer, “Towards Information-Theoretic Security in Optical Networks Basics of Physical-Layer Security,” in Photonic Networks; 18. ITG-Symposium, 2017, pp. 64–70. Citado 1 vez na página 16.

[19] K. Kravtsov, Z. Wang, W. Trappe, and P. R. Prucnal, “Physical layer secret key generation for fiber-optical networks,” Opt. Express, vol. 21, no. 20, p. 23756, 2013. Citado 1 vez na página 16.

[20] A. A. E. Hajomer, X. Yang, A. Sultan, W. Sun, and W. Hu, “Key Generation and Distribution Using Phase Fluctuation in Classical Fiber Channel,” 20th Int. Conf. Transparent Opt. Networks, 2018-July, pp. 2018–2020, 2018. Citado 1 vez na página 16.

[21] L. M. Pecora and T. L. Carroll, “Synchronization in Chaotic Systems,” Phys. Rev. Lett., vol. 64, no. 8, pp. 821–825, 1990. Citado 1 vez na página 17.

[22] L. M. Pecora and T. L. Carroll, “Driving systems with chaotic signals,” Phys. Rev. A, vol. 44, no. 4, pp. 2374–2383, 1991. Citado 1 vez na página 17.

[23] L. M. Pecora and T. L. Carroll, “Synchronization of chaotic systems,” Chaos, vol. 25, no. 9, 2015. Citado 1 vez na página 17.

[24] A. Zhao, N. Jiang, S. Liu, Y. Zhang, and K. Qiu, “Generation of synchronized wideband complex signals and its application in secure optical communication,” Opt. Express, vol. 28, no. 16, p. 23363, 2020. Citado 1 vez na página 17.

[25] S. Liu, N. Jiang, A. Zhao, Y. Zhang, and K. Qiu, “Secure Optical Communication Based on Cluster Chaos Synchronization in Semiconductor Lasers Network,” IEEE Access, vol. 8, pp. 11872–11879, 2020. Citado 1 vez na página 17.

[26] L. Yi, T. Zhang, Z. Li, J. Zhou, Y. Dong, and W. Hu, “Secure optical communication using stimulated Brillouin scattering in optical fiber,” Opt. Commun., vol. 290, pp. 146–151, 2013. Citado 1 vez na página 17

[27] D. Wang, Z. Wu, M. Zhang, and X. Tang, “Multifunctional all-optical signal processing scheme for wavelength-division-multiplexing multicast, wavelength conversion, format conversion, and all-optical encryption using hybrid modulation format exclusive-OR gates based on four-wave mixing in highly,” Appl. Opt., vol. 57, no. 7, p. 1562, 2018. Citado 1 vez na página 17

[28] X. Chen, L. Huo, Z. Zhao, L. Zhuang, and C. Lou, “Reconfigurable all-optical logic gates using single semiconductor optical amplifier at 100-Gb/s,”

IEEE Photonics Technol. Lett., vol. 28, no. 21, pp. 2463–2466, 2016. Citado 1 vez na página 17..

[29] J. A. Cornejo, C. E. Perez, and J. L. de Bougrenet de la Tocnaye, “WDM-compatible channel scrambling for secure high-data-rate optical transmissions,” J. Light. Technol., vol. 25, no. 8, pp. 2081–2089, 2007.Citado 1 vez na página 18.

[30] M. L. F. Abbade, M. Cvijetic, C. A. Messani, C. J. Alves, and S. Tenenbaum, “All-optical cryptography of M-QAM formats by using two-dimensional spectrally sliced keys,” Appl. Opt., vol. 54, no. 14, p. 4359, 2015. Citado 1 vez na página 18.

[31] M. L. F. Abbade, L. D. B. Bobadilla, D. O. De Carvalho, A. A. Ferreira, L. H. Bonani, and I. Aldaya, “All-optical encryption using multi-channel spectral shuffling,” IEEE Photonics Technol. Lett., vol. 31, no. 1, pp. 98–101, 2019. Citado 1 vez na página 18

[32] T. De Andrade Bragagnolle, M. P. Nogueira, M. O. Santos, A. J. Do Prado, A. A. Ferreira, E. A. De Mello Fagotto, I. Aldaya, M. L. F. Abbade “All-optical spectral shuffling of signals traveling through different optical routes,” in International Conference on Transparent Optical Networks, 2019, vol. 2019-July. Citado 1 vez na página 18

[33] M. De Oliveira Santos, W. S. Souza, T. De Andrade Bragagnolle, L. D. B. Bombadilla, I. Aldaya, A. J. Do Prado, A. A. Ferreira, L. H. Bonani, M. L. F. Abbade “All-optical Spectral Shuffling Applied to 16-QAM Signals,” in 2019 SBFoton International Optics and Photonics Conference, SBFoton IOPC 2019, 2019. Citado 1 vez na página 18

[34] A. K. Khandani and E. Bateni, “A Practical, Provably Unbreakable Approach to Physical Layer Security,” in 2019 16th Canadian Workshop on Information Theory, CWIT 2019, 2019, pp. 1–6. Citado 1 vez na página 19.

[35] T. Kodama, “Digital-domain dual encryption key-based phase shift symbol masking with cascaded encoder/decoder for secure coherent optical systems,” Opt. InfoBase Conf. Pap., vol. Part F138-, pp. 2019–2021, 2019. Citado 1 vez na página 19.

[36] M. L. F. Abbade, M. P. Nogueira, M. O. Santos, E. A. M. Fagotto, L. H. Bonani, and I. Aldaya, “DSP-Based Multi-Channel Spectral Shuffling Applied to Optical Networks,” IEEE Photonics Technol. Lett., vol. 32, no. 3, pp. 154–157, 2020. Citado 1 vez na página 19.

[37] W. S. Souza et al., “Spectral Shuffling with Phase Encoding and Dynamic Keys Applied to Transparent Optical Network Signals,” in 22nd International Conference on Transparent Optical Networks, 2020, p. Th.A2.3.1 a Th.A2.3.4. Citado 2 vezes na página 19.

[38] X. Hu, X. Yang, Z. Shen, H. He, W. Hu, and C. Bai, “Chaos-Based Partial Transmit Sequence Technique for Physical Layer Security in OFDM-PON,” IEEE Photonics Technol. Lett., vol. 27, no. 23, pp. 2429–2432, 2015. Citado 2 vezes na página 19.

[39] W. Zhang, C. Zhang, C. Chen, H. Zhang, W. Jin, and K. Qiu, “Hybrid Chaotic Confusion and Diffusion for Physical Layer Security in OFDM-PON,” IEEE Photonics J., vol. 9, no. 2, pp. 1–10, 2017. Citado 2 vezes na página 19.

[40] A. A. E. Hajomer, X. Yang, and W. Hu, “Secure OFDM Transmission Precoded by Chaotic Discrete Hartley Transform,” IEEE Photonics J., vol. 10, no. 2, pp. 1–9, 2018. Citado 2 vezes na página 19.

[41] Y. Xiao et al., “Two-level encryption for physical-layer security in OFDM-PON based on multi-scrolls system,” Opt. Commun., vol. 440, no. December 2018, pp. 126–131, 2019. Citado 2 vezes na página 19.

[42] Y. Wang, W. Zhang, G. Chen, X. Yang, and W. Hu, “Multi-Gbit/s real-time modems for chaotic optical OFDM data encryption and decryption,” Opt. Commun., vol. 432, no. July 2018, pp. 39–43, 2019. Citado 2 vezes na página 19.

[43] Ngo, H. H.; Wu, X.; Le, P. D.; Wilson, C.; Srinivasan, B. “Dynamic Key Cryptography and Applications,” International Journal of Network Security, v. 10, n. 3, May 2010. Citado 1 vez na página 19.

[44] A. J. Menezes, J. Katz, P. C. Van Oorschot, and S. A. Vanstone. “Handbook of applied cryptography,” CRC press, 1996. Citado 2 vezes nas páginas 22 e 23.

[45] D. J. Wheeler and R. Needham, “TEA, a Tiny Encryption Algorithm,” Computer Laboratory, Cambridge University, England. November, 1994. Citado 3 vezes nas páginas 23, 24 e 25.

[46] N. F. PUB, “46-3. Data Encryption Standard,” Federal Information Processing Standards, National Bureau of Standards, US Department of Commerce, 1977. Citado 1 vez na página 25.

[47] C. E. Shannon, “Communication Theory of Secrecy Systems,” Bell system technical journal, vol. 28, no. 4, pp. 656–715, 1949.Citado 1 vez na página 25.

[48] W. Diffie and M. E. Hellman, "Privacy and authentication: An introduction to cryptography," in Proceedings of the IEEE, vol. 67, no. 3, pp. 397-427, March 1979. Citado 1 vez na página 26.

[49] H. LIPMAA, D. WAGNER, P. ROGAWAY, "Comments to NIST concerning AES Modes of Operations: CTR-Mode Encryption," pp. 1-4, September 2000. Citado 2 vezes na página 27.

[50] M. L. F. Abbade; I. Aldaya ; M. O. Santos ; M. P. Nogueira ; W. S. Souza. KryptoSJ v03. 2019. Citado 1 vez na página 31.

[51] M. de Oliveira Santos, “Criptografia na camada física baseada em codificação espectral implantada por meio de DSP e aplicada a redes ópticas,” Mestrado em Engenharia Elétrica, Universidade Estadual Paulista (UNESP), São João da Boa Vista, 2020. Citado 1 vez na página 31.

[52] W. S. Souza, “Adaptação de Criptografia Espectral ao Paradigma do Advanced Encryption Standard,” Mestrado em Engenharia Elétrica, Universidade Estadual Paulista (UNESP), São João da Boa Vista, 2020. (Dissertação em desenvolvimento). Citado 1 vez na página 31.

[53] B. P. Lathi; Z. Ding, “Sistemas de Comunicações Analógicas e Digitais Modernos,” LTC, 2012.Citado 1 vez na página 31.